



iboss Secure Web Gateway

User Manual

Note: Please refer to the User Manual online for the latest updates at www.iboss.com.

Copyright © by iboss, Inc. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in chemical, manual or otherwise, without the prior written permission of iboss, Inc.

iboss Network Security makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defects. Further, this company reserves the right to revise this publication and make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

www.iboss.com

Open Source Code

This product may include software code subject to the GNU General Public License ("GPL"), GNU Lesser General Public License ("LGPL"), or other open-source software licenses. Copies of the GPL and LGPL licenses are available upon request. You may also visit www.gnu.org to view more information regarding open-source licensing.

The GPL, LGPL and other open-source code used in iboss, Inc. products are distributed without any warranty and are subject to the copyrights of their authors. Upon request, open-source software source code is available from iboss, Inc. via electronic download or shipment on a physical storage medium at cost. For further details and information please visit www.iboss.com/.

Table of Contents

1	IBOSS ENTERPRISE WEB FILTER	15
1.1	OVERVIEW	15
1.2	KEY FEATURES	15
1.3	MANUAL STRUCTURE	15
1.4	SYSTEM REQUIREMENTS	16
2	SPECIFICATIONS	17
2.1	IBOSS ENTERPRISE SWG MODEL SPECIFICATIONS	17
2.2	FRONT PANEL & BACK PANELS	18
2.2.1	Ethernet Ports	18
2.2.2	Console Port	18
2.2.2.1	Console Port Settings	18
3	GETTING STARTED	19
3.1	OPERATION MODE OVERVIEW	19
3.1	IBOSS NETWORK SETTINGS CONFIGURATION	20
3.1.1	Configuring Network Settings via Serial Console	20
3.1.2	Configuring Network Settings via the Network	21
3.1.2.1	Configuring Network Settings via iboss User Interface	21
4	INTERFACE	22
4.1	DASHBOARD	22
4.2	WIDGETS	22
4.2.1	Filtering Status	22
4.2.2	Quick Links	23
4.2.3	Bandwidth Shaping Pools	23
4.2.4	Firmware	23
4.2.5	URL Lookup	23
4.3	MAIN MENU	23

4.4	TOP SHORTCUT BAR	24
5	NETWORK MENU SETTINGS	25
5.1	CONFIGURE INTERNET CONNECTION.....	27
5.1.1	<i>Basic Configuration</i>	27
5.1.2	<i>Inline or Tap</i>	28
5.1.3	<i>Remote Authentication Integration</i>	28
5.1.4	<i>Internal Report Manager Listen Port</i>	29
5.1.5	<i>Status</i>	29
5.2	GATEWAY SSL DECRYPTION	29
5.2.1	<i>Overview</i>	29
5.2.2	<i>Understanding HTTPS/SSL Decryption</i>	30
5.2.2.1	<i>The HTTPs/SSL Protocol</i>	30
5.2.3	<i>General Settings</i>	32
5.2.4	<i>User SSL Decryption Alert</i>	33
5.2.5	<i>SSL Decryption IP Address Bypass</i>	37
5.2.6	<i>Selective SSL Decryption</i>	37
5.2.7	<i>Additional SSL Decryption DNS Servers</i>	38
5.2.8	<i>Conclusion</i>	39
5.3	SSL CERTIFICATE SETTINGS	40
5.4	BYOD SETTINGS	40
5.5	SNMP SETTINGS	41
5.6	LDAP SETTINGS	42
5.6.1	<i>Global Settings</i>	42
5.6.2	<i>Add LDAP Server</i>	43
5.6.2.1	<i>Match Active Directory Groups with iboss Filtering Groups</i>	45
5.7	ACTIVE DIRECTORY & PROXY SETTINGS	46
5.7.1	<i>Settings</i>	46

5.7.2	<i>Proxy Cache Settings</i>	49
5.7.2.1	Proxy Mobile Devices (Source IP).....	49
5.7.2.2	Automatic GPO Setup for NTLM with Login/Logoff Scripts.....	50
5.8	ACTIVE DIRECTORY PLUGIN/NETWORK ACCESS CONTROLLER INTEGRATION	56
5.8.1	<i>Global Settings</i>	57
5.8.2	<i>Last Communication Info</i>	58
5.8.3	<i>Registered AD Servers / NAC Agents</i>	58
5.8.3.1	Stats	58
5.8.4	<i>Add Active Directory Server</i>	59
5.8.5	<i>iboss Active Directory Plugin Configuration</i>	60
5.8.5.1	Edit AD Plugin Orca.....	62
5.8.5.2	AD Plugin Radius Audit Log	63
5.8.5.3	Active Directory Audit Logon Events.....	64
5.8.5.4	NAC Integration.....	66
5.9	MOBILE CLIENT & LOCAL SSL INSPECTION AGENT	66
5.10	IBOSSNETID SINGLE SIGN-ON AGENT.....	68
5.11	eDIRECTORY SETTINGS.....	69
5.11.1	<i>iboss eDirectory Transparent Integration</i>	69
5.11.1.1	Overview	70
5.11.2	<i>Global Settings</i>	70
5.11.3	<i>eDirectories</i>	71
5.11.4	<i>Insert eDirectory – Server Registration Settings</i>	72
5.12	CLUSTERING	75
5.12.1	<i>Local Settings</i>	76
5.12.2	<i>Cluster Members</i>	76
5.12.3	<i>Add Cluster Member</i>	77
5.13	ADD ADDITIONAL ROUTES	78
5.14	BYPASS IP RANGES.....	80

5.15	BYPASS INTERFACE	81
5.16	ADD ADDITIONAL LOCAL SUBNETS	82
5.16.1	Overview	82
5.16.2	Insert Local Subnets/IP Ranges	84
5.17	REGISTER INTERNAL GATEWAYS	85
5.17.1	Overview	86
5.17.2	Global Settings	86
5.17.3	Insert Internal Gateway	87
5.18	EDIT ADVANCED NETWORK SETTINGS	88
5.18.1	General Settings	88
5.18.2	Group Cache Settings	89
6	INSTALLING THE IBOSS ON THE NETWORK	89
6.1	TRANSPARENT INLINE BRIDGE	89
7	THREAT CONSOLE	90
7.1	REPORT SETTINGS	90
7.1.1	General Settings	90
7.1.2	Log Web Statistics	91
7.1.3	Additional Settings	92
7.2	URL PATTERN IGNORE LIST	93
7.3	REPORTER	93
8	CONFIGURE CONTROLS	94
8.1.1	Web / SSL Categories	96
8.1.1.1	Category Scheduling	96
8.1.1.2	Additional Settings	97
8.1.1.3	Categories	98
8.1.1.4	Identify Theft (Phishing)/ IP Address Blocking Page	99
8.1.2	Application Management	100
8.1.2.1	Chat Applications	100

8.1.2.2	Gaming Applications.....	101
8.1.2.3	File Sharing Applications.....	102
8.1.2.4	Ultrasturf / Tor / High-Risk Activity Device Lock	103
8.1.2.5	Additional Settings	104
8.1.3	<i>Advanced Social Media & Web 2.0 Controls.....</i>	105
8.1.3.1	Social Chat App Controls	105
8.1.3.2	Social Streaming Radio Controls.....	106
8.1.3.3	Pinterest Controls	106
8.1.3.4	Facebook Controls	107
8.1.3.5	Twitter Controls.....	108
8.1.3.6	Linked-in Controls	108
8.1.3.7	Encrypted Search Controls.....	109
8.1.3.8	YouTube & Video Controls.....	109
8.1.3.9	Google Controls	110
8.1.3.10	Gmail Controls	111
8.1.4	<i>Allowlist.....</i>	112
8.1.4.1	Preferences	112
8.1.4.2	Allowlist	113
8.1.4.3	Custom Allow list Categories.....	114
8.1.4.4	Allowlist Import	115
8.1.5	<i>Block Specific Websites</i>	116
8.1.5.1	Custom Block list Categories.....	117
8.1.5.2	Block list Import	118
8.1.6	<i>Keyword Blocklist/Allowlist.....</i>	119
8.1.6.1	Pre-Defined Keyword Lists	119
8.1.6.2	Keywords	119
8.1.6.3	Keyword Import.....	120
8.1.7	<i>Bandwidth Shaping.....</i>	121

8.1.8	Port Blocking.....	122
8.1.9	Content/MIME Type Restrictions	123
8.1.10	File Extension Blocking.....	124
8.1.11	Domain Extension Restrictions	124
8.1.12	Sleep Schedule.....	125
8.1.12.1	Sleep Mode Page	126
8.1.13	Real-Time Monitoring/Recording.....	127
8.1.14	Exception Requests.....	129
8.1.15	URL Lookup	130
9	PREFERENCES.....	131
9.1.1	System Settings.....	132
9.1.2	Block Pages.....	133
9.1.2.1	Blocked Page.....	133
9.1.2.2	Sleep Mode Page	134
9.1.2.3	DNS Block Response IP	134
9.1.2.4	Redirect Source MAC Address (Global)	135
9.1.2.5	Block Page	135
9.1.3	Remote Management.....	136
9.1.4	User Settings.....	136
9.1.4.1	Group User Settings.....	137
9.1.4.2	Global User Settings.....	139
9.1.4.1	User Internet Access Window	141
10	GROUPS.....	142
10.1	FILTERING GROUPS	143
10.1.1	Edit Filtering Group.....	144
10.1.2	Copy Group Settings	145
10.1.3	Group – Computers & Users Tabs	146
10.1.1	Add User.....	147

10.1.1.1	General	148
10.1.1.2	Delegation.....	148
10.1.1.3	Time Limits	149
10.1.2	<i>Add Computer.....</i>	<i>150</i>
11	TOOLS	151
11.1	BACKUP & RESTORE MANAGER	151
11.2	CLEAR INTERNAL CACHES	154
11.3	CLEAR DNS CACHES	154
11.4	TRIGGER MDM SYNC.....	154
12	FIRMWARE UPDATES	155
13	SUBSCRIPTION.....	156
14	SUPPORT	156
15	TROUBLESHOOTING.....	156
15.1	PASSWORD RECOVERY	156
15.2	RESETTING TO FACTORY DEFAULTS.....	156
15.2.1	<i>Through the iboss User Interface</i>	<i>157</i>
15.2.2	<i>Using the iboss Console Port.....</i>	<i>157</i>
15.3	TECHNICAL SUPPORT	157
16	APPENDIX.....	157
16.1	TERMS OF USE	157
17	REGULATORY STATEMENT	157

Table of Figures

Table 1 – Serial Console Port Settings.....	18
Figure 1 – COM Properties	19
Table 2 – Default iboss IP Address Settings.....	20
Table 3 – Computer IP Address settings used to initially configure iboss through the network .	21
Figure 2 – Home Page	22
Figure 3 – Network Menu.....	25
Figure 4 – Internet Connection.....	27
Figure 5 – Internet Connection – Basic Configuration.....	27
Figure 6 – Internet Connection – Inline or Tap	28
Figure 7 – Internet Connection – Remote Authentication Integration	28
Figure 8 – Internet Connection – Internal Report Manager Listen Port	29
Figure 9 – Internet Connection – Status.....	29
Figure 10 – Internet Explorer Certificate Warning	31
Figure 11 – Firefox Certificate Warning	31
Figure 12 – Gateway SSL Decryption – General Settings	32
Figure 13 – Gateway SSL Decryption – User SSL Decryption Alert.....	33
Figure 14 – User Alert When Visiting SSL Intercepted Domain	34
Figure 15 – Gateway SSL Decryption – SSL Decryption IP Address Bypass	37
Figure 16 – Gateway SSL Decryption – Selective SSL Decryption	37
Figure 17 – Gateway SSL Decryption – Additional SSL Decryption DNS Servers	38
Figure 18 – SSL Settings	40
Figure 19 – BYOD Settings	40
Figure 6 – SNMP Settings.....	41
Figure 20 – LDAP Settings.....	42

Figure 21 – LDAP Settings – Add LDAP Server	43
Figure 22 – Active Directory & Proxy Settings.....	46
Figure 23 – GPO Default Domain Policy.....	51
Figure 24 – GPO Connection Settings.....	52
Figure 25 – GPO Import the Connection Settings.....	52
Figure 26 – GPO Use Proxy Server	53
Figure 27 – GPO Local Area Network Settings	54
Figure 28 – Manual Proxy with Internet Explorer	55
Figure 29 – Manual Proxy with Mozilla Firefox	55
Figure 30 – AD Plugin / NAC Integration	56
Figure 31 – AD Plugin – Global Settings	57
Figure 32 – AD Plugin – Last Communication Info	58
Figure 33 – AD Plugin – Add Active Directory Server	59
Figure 34 – iboss Active Directory Plugin Configuration	60
Figure 35 – Edit with Orca option	62
Figure 36 – AD Plugin Properties with Orca	63
Figure 37 – AD Plugin Radius Audit Log Configuration	64
Figure 38 – Domain Security Policy.....	64
Figure 39 – Audit Account Logon Events	65
Figure 40 – Audit Logon Events.....	65
Figure 41 – Mobile Client & Local SSL Inspection Agent	66
Figure 42 – Mobile Client & Local SSL Inspection Agent 2	67
Figure 43 – ibossNetID Single Sign-On Agent	68
Figure 44 – eDirectory Settings	69
Figure 45 – Insert eDirectory	72
Figure 46 – Clustering.....	75

Figure 47 – Clustering – Add Cluster Member	77
Figure 48 – Add Additional Routes	78
Figure 49 – Bypass IP Range.....	80
Figure 50 – Bypass Interface Configuration	81
Figure 51 – Add Additional Local Subnets.....	82
Figure 52 – Insert Local Subnet.....	84
Figure 53 – Register Internal Gateways	85
Figure 54 – Insert Internal Gateway	87
Figure 55 – Edit Advanced Network Settings	88
Figure 56 – iboss Hardware Installation	89
Figure 57 – Report Settings – General Settings.....	90
Figure 58 – Report Settings – Log Web Statistics.....	91
Figure 59 – Report Settings – Additional Settings	92
Figure 60 – Report Settings – URL Pattern Ignore List	93
Figure 61 – Configure Internet Controls Menu	94
Figure 62 – Web/SSL Categories	96
Figure 63 – Category Scheduling	96
Figure 64 – Category Example.....	98
Figure 65 – Application Management	100
Figure 66 – Applications – Chat Applications	100
Figure 67 – Applications – Gaming Applications	101
Figure 68 – Applications – File Sharing Applications	102
Figure 69 – Ultrasurf / Tor / High-Risk Activity Device Lock	103
Figure 70 – Application – Additional Settings	104
Figure 71 – Advanced Social Media & Web 2.0 Controls	105
Figure 72 – Social Chat App Controls	105

Figure 73 – Social Streaming Radio Controls	106
Figure 74 – Pinterest Controls	106
Figure 75 – Facebook Controls	107
Figure 76 – Twitter Controls.....	108
Figure 77 – Linked-in Controls	108
Figure 78 – Encrypted Search Controls	109
Figure 79 – YouTube & Video Controls.....	109
Figure 80 – Google Controls.....	110
Figure 81 – Gmail Controls.....	111
Figure 82 – Allowlist	112
Figure 83 – Custom Allow list Categories.....	114
Figure 84 – Allowlist Import	115
Figure 85 – Block Specific Websites	116
Figure 86 – Custom Block list Categories.....	117
Figure 87 – Block list Import	118
Figure 88 – Keyword Blocklist/Allowlist	119
Figure 89 – Keyword Import	120
Figure 90 – Bandwidth Throttling	121
Figure 91 – Port Blocking	122
Figure 92 – Block Content/MIME Types.....	123
Figure 93 – File Extension Blocking.....	124
Figure 94 – Domain Extensions Restrictions	124
Figure 95 – Sleep Schedule	125
Figure 96 – Real-time Monitoring/Recording	127
Figure 97 – Exception Requests.....	129
Figure 98 – URL Exception Request – Block Page	129

Figure 99 – URL Lookup.....	130
Figure 100 – Preferences	131
Figure 101 – System Settings.....	132
Figure 102 – Customize Block Pages.....	133
Figure 103 – Customize Block Pages – Block Page.....	133
Figure 104 – Customize Block Pages – Sleep Mode Page.....	134
Figure 105 – Customize Block Pages – DNS Block Response IP.....	134
Figure 106 – Customize Block Pages – Redirect Source MAC Address.....	135
Figure 107 – iboss Block Page	135
Figure 108 – Remote Management.....	136
Figure 109 – User Settings – Group User Settings.....	137
Figure 110 – User Settings – Global User Settings	139
Figure 111 – Internet Access Window Login.....	141
Figure 112 – Internet Access Window Session.....	141
Figure 113 – Groups	142
Figure 114 – Filtering Group Menu.....	142
Figure 115 – Filtering Groups	143
Figure 116 – Edit Group.....	144
Figure 117 – Groups – Copy Group Settings.....	145
Figure 118 – Copy Group Icon.....	145
Figure 119 – Group – Computers & Users Tabs	146
Figure 120 – Add User	147
Figure 121 – Users – Delegation.....	148
Figure 122 – Users – Time Limits.....	149
Figure 123 – Add Computer	150
Figure 124 – Tools.....	151

Figure 125 – Backup & Restore Manager Login.....	151
Figure 126 – Backup & Restore – Restore Points & Creating Restore Point	152
Figure 127 – Automated Scheduled Backup.....	153
Figure 128 – Restore Settings	154
Figure 129 – Firmware Updates.....	155
Figure 130 – Subscription	156

1 iboss Enterprise SWG Filter

1.1 Overview

The iboss Enterprise SWG is a line of web filters for medium to large networks. Powerful patent-pending filtering technology puts you in control of Internet usage on your network. Flexible Internet controls allow you to easily restrict access to specific categories of Internet destinations and manage time spent using online programs (online chat and messenger programs, file sharing, gaming and more). It utilizes an industry first advanced real-time graphical user interface, robust Internet traffic controls, total network traffic analyzer, up to the second network activity feed MRTG, and a live real-time URL database feed ensuring the most accurate filtering possible.

1.2 Key Features

- **Comprehensive Web Filtering**
- **Application Firewall**
- **QoS/Bandwidth Shaping**
- **Policy Scheduling**
- **Robust Reports**
- **Real-Time MRTG**
- **Remote Management**
- **Individual User Login with LDAP/Active Directory Integration**
- **Policies Users/Groups**
- **Real-Time URL Updates**
- **Simple & User-Friendly Interface**
- **Plug & Play with No Software to Install**
- **Compatible with any Operating System**

1.3 Manual Structure

This manual includes detailed information and instructions for installing and configuring the iboss. The **"Getting Started"** section of this manual will guide you through the initial hardware installation and setup

process. The “**Configuration**” section of the manual contains detailed instructions for configuring specific settings and customizing preferences.

Note: For quick installation instructions, you may also reference the iboss Quick Installation Guide included with the product.

1.4 System Requirements

- Broadband (Cable, DSL, T1, FiOS, Fiber, etc.) Internet service
- Network Adapter for each computer
- Existing Firewall and Switch
- Any Major Operating System running a TCP/IP network (i.e. Mac, Windows, Linux, etc.)
- Standard Web Browser
- Active iboss Subscription

2 Specifications

2.1 iboss Enterprise SWG Model Specifications

The iboss Enterprise SWG has the following specifications & onboard report settings:

Model	Recommended Concurrent Users	Identifiable Computers	Identifiable Users	Filtering Groups	Reports Database Size	Generated Reports	Report Schedules
1560	50–100	120	120	25	25 GB	50	5
1760	101–200	240	240	50	25 GB	75	10
2160	201–300	360	360	60	25 GB	75	10
2560	301–400	480	480	75	25 GB	100	15
3560	401–600	720	720	100	25 GB	100	20
4560	601–1000	1200	1200	125	25 GB	125	25
5560	1001–1500	1800	1800	200	25 GB	250	30
6560	1501–2000	2400	2400	300	25 GB	300	35
7560	2001–2500	3600	3600	100	25 GB	300	35
8560	2501–4000	4800	4800	300	25 GB	300	35
9560	4001–6000	7200	7200	300	25 GB	300	35
10600	6001–12,000	7200	7200	300	25 GB	300	35
14600	12,001–50,000	7200	7200	300	25 GB	300	35
14600x	50,000–100,000	7200	7200	300	25 GB	300	35
16600	12,001–50,000	7200	7200	1000	25 GB	300	35

2.2 Front Panel & Back Panels

2.2.1 Ethernet Ports

The back panel contains two Fast Ethernet 10/100/1000 Mbps ports. The following provides a description for each port:

LAN – The port labeled “LAN” should be connected to your local area network. Typically, this port is connected to the switch on your LAN that is connected to all of the filtered computers on the network.

WAN – The port labeled “WAN” should be connected to an Internet accessible connection. Typically, this port is connected to your firewall/router.

Bypass (Fail-Safe) Ports (not in all versions) – These ports are fail-safe ports which will be used instead of using the default ports. It is used for fail-safe features.

Management Port – The port labeled “Management Interface” should be connected to your switch. This is the port which the IP address resides on and gives access to the SWG interface.

2.2.2 Console Port

The Console port provides a serial RS–232 interface to the iboss. This port provides such functions such as configuring the network settings for the iboss, displaying the IP Address settings for the iboss, and restoring factory defaults. When using directly to a computer you must use a NULL MODEM DB9 serial cable.

This port can be accessed via any console (COM) program. On windows, you can use the built-in program HyperTerminal. Other console programs that are available include PuTTY.

2.2.2.1 Console Port Settings

The settings for the console port are as follows:

Table 1 – Serial Console Port Settings

Bits Per Second	19200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

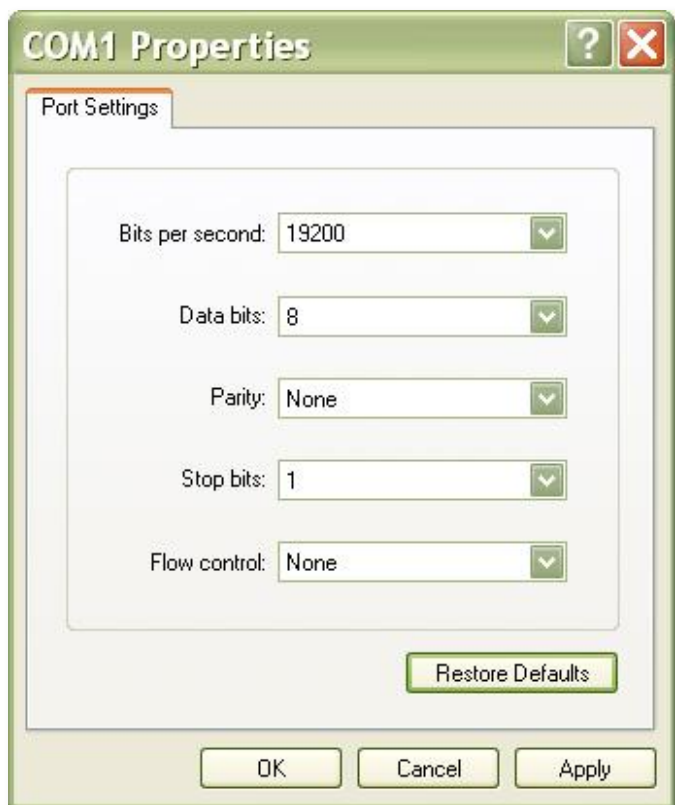


Figure 1 – COM Properties

3 Getting Started

This section describes initial setup and configuration of the iboss appliance. This section contains information that will help you install the iboss onto your network.

3.1 Operation Mode Overview

The iboss provides its filtering functionality in a completely transparent fashion on the network. It does not segment a network, nor does it provide firewall or NAT capability. The iboss filters traffic passing between the LAN and WAN port. The iboss will actively scan traffic applying filtering rules and intercepting traffic when necessary. This allows the iboss to achieve very high filtering performance without affecting network topology.

In order for the iboss to perform filtering, it must be configured to have its own IP Address on the local network. The IP Address must be a static IP Address that is available on the network. Before connecting the iboss to the network, the IP Address settings must be configured to match the network it is being installed on.

Once the address is configured, you will be able to access the iboss while on the local network by entering the IP Address that was configured into the iboss into your Web Browser (Default 192.168.1.10).

3.1 iboss Network Settings Configuration

Before the iboss can be connected to the network, the IP Address settings that the iboss will use must be configured. The iboss must be configured with a static IP Address and will not obtain an IP Address through DHCP.

The iboss ships with the following default IP Address settings. If these settings are sufficient for the network where it is being installed, you may not need to adjust the IP Address settings and skip this process.

Table 2 – Default iboss IP Address Settings

IP Address	192.168.1.10
Subnet Mask	255.255.255.0
Gateway	192.168.1.1
DNS 1	192.168.1.1
DNS 2	0.0.0.0

There are two methods for configuring the IP Address settings of the iboss. The first method involves using the serial console port. The second method involves connecting a single computer to the iboss LAN port and configuring via the network using your Web Browser. If you have the external Report Manager, the default IP address is 192.168.1.20 for the external Enterprise Reporter.

3.1.1 Configuring Network Settings via Serial Console

To configure the network settings via the console terminal, connect the provided serial cable to the console port on the iboss. After the iboss has been powered on (typically full boot-up takes between 3–4 minutes), open a serial console program. On windows, you can use the built-in HyperTerminal program to access the console port.

The settings for the serial console COM connection are shown in the hardware specifications and are re-listed below:

Bits Per Second	19200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

Once you have connected the serial cable from your computer to the console port and configured the console program, press the <Enter> key repeatedly until the configuration menu is displayed. Follow the options presented to configure the static IP Address settings for the iboss.

3.1.2 Configuring Network Settings via the Network

You can also configure the iboss network settings by connecting to the iboss via a Web Browser. The following instructions apply when initially configuring the iboss IP Address settings. If you have already configured the IP Address settings and wish to change them, you need to log into the iboss using its current IP Address settings.

In order to do this, you must configure your computer to have a static IP address within the subnet of the iboss default network settings. Configure your computer to have the following static IP Address:

Table 3 – Computer IP Address settings used to initially configure iboss through the network

IP Address	192.168.1.15
Subnet Mask	255.255.255.0

You can leave the Gateway and DNS IP Address blank on your computer as they will not be needed.

With these settings in place, open a web browser and enter 192.168.1.10 into your Web Browser's address bar. This will bring up the iboss home page. From the homepage, follow the Setup Internet Connection link to configure the iboss IP Address Settings.

3.1.2.1 Configuring Network Settings via iboss User Interface

The iboss does not require any software installation. Instead, its user interface can be accessed directly using a standard Internet web browser. The web-based user interface allows you to configure your iboss.

1. Verify that your computer has an IP address that is on the same subnet as the iboss IP address, as stated above.
2. Open a standard Internet web browser application (Internet Explorer®, Firefox®, etc.).
3. In the URL address bar, enter the IP address of <http://192.168.1.10> and press <enter>. This will take you to the iboss interface.

Note: The management interface is built into the iboss, so it is always accessible even though the Internet may not be. You may access the user interface from any computer connected behind the iboss.

4 INTERFACE

4.1 Dashboard

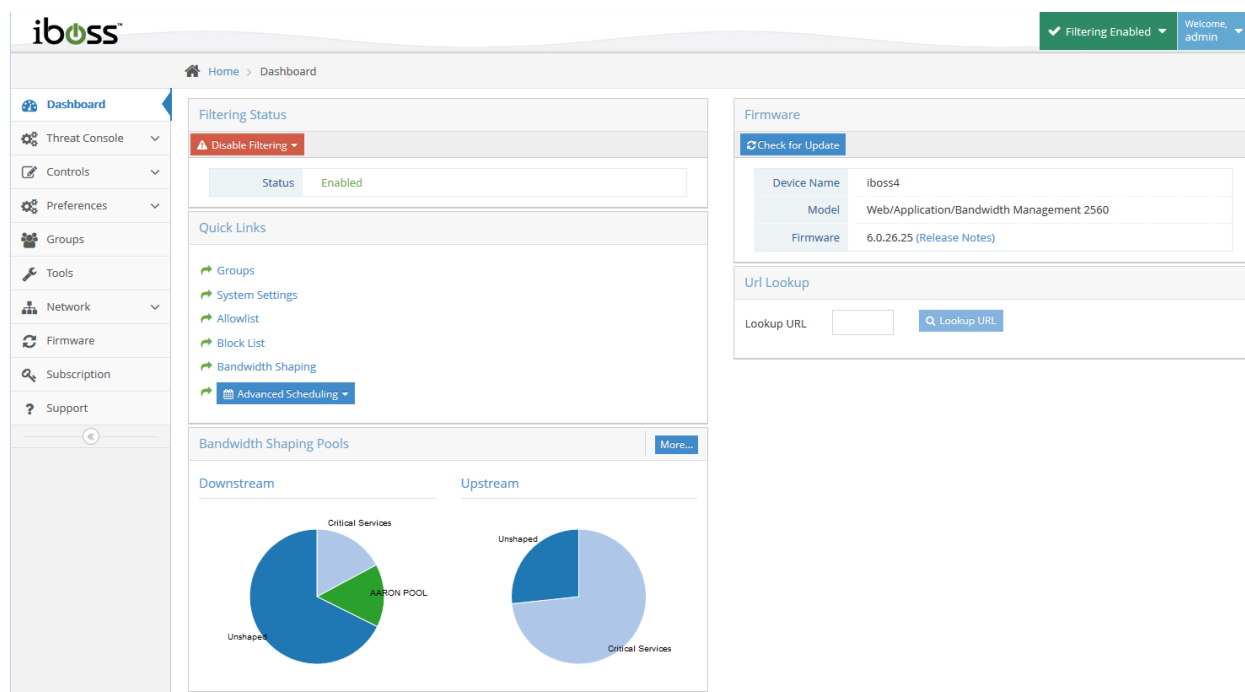


Figure 2 – Home Page

4.2 Widgets

4.2.1 Filtering Status

This indicates the filtering status of your iboss. The following values may be displayed:

Enabled – Indicates that your iboss is Enabled and Active.

Disabled – Indicates that your iboss is not enabled.

Connecting – When the iboss is enabled, it must first establish a connection to the gateway.

This indicates that the iboss is attempting to establish a connection.

Must Activate or Subscription Expired – If you have a new iboss and need to activate your subscription, or your iboss subscription has expired, the "Activate" button will appear next to the filtering status field. Click the "Activate" button to proceed with your iboss activation.

Current Date & Time – Indicates the current date and time. The date and time are synchronized when the iboss establishes a connection to the gateway, and are important for performing Internet scheduling and report logging. The local time zone settings may be set from the "Edit My Time Zone" page under "My Preferences".

Note: The date & time will only be displayed when the iboss status is “Enabled”.

Enable/Disable Filtering Button – The “Enable/Disable” button is located above to the Filtering Status field. It is useful for quickly enabling and disabling your iboss filtering. If your status reads “Not Enabled”, clicking the “Enable” button will enable filtering. You may also choose to Disable for time periods such as 15 Min, 30 Min, 1 Hour, 2 Hours, 12 Hours, 24 Hours or Until Re-enabled.

4.2.2 Quick Links

This section provides links to common sections within the SWG interface.

4.2.3 Bandwidth Shaping Pools

This section provides a quick view of the current bandwidth pools.

4.2.4 Firmware

This section displays model and Firmware Version allowing for quick update actions.

4.2.5 URL Lookup

This section allows you to quickly lookup a URL on which categories it falls under.

4.3 Main Menu

The “**Home**” menu allows you to choose options for configuring the current iboss settings. These are options to choose from: **Dashboard, Threat Console, Controls, Preferences, Groups, Tools, Network, Firmware, Subscription, and Support.**

Dashboard – This option allows you to view status of the filtering and firmware version as well as quick links and tools that are most useful.

Threat Console – This option allows you to view your iboss report logs and configure settings for the Threat Console.

Controls – This section allows you to configure filtering policies for existing groups.

Preferences – This section allows you to edit preferences including E-mail options, Web GUI password, time zone and custom block messages.

Groups– This section allows you to identify computers and users on the network, as well as create filtering groups. This is also where you would create delegated administrators with the ability login to the iboss and access some or all portions of the User Interface.

Tools – This section is where to clear internal/DNS caches for the iboss and access the Backup & Restore menu. This is also where to trigger Filter-to-MDM synchronization if necessary.

Network – This section allows you to configure your iboss network settings.

Firmware – This section includes all firmware information for the iboss and allows you to update the firmware when updates are available.

Subscription – This page allows you to view your subscription status and add or update a Subscription Key.

Support – This page allows you to access information for support for the iboss SWG.

4.4 Top Shortcut Bar

Use the top right shortcut menu to Disable Filtering as well as changing the admin password and logging out.

5 Network Menu Settings

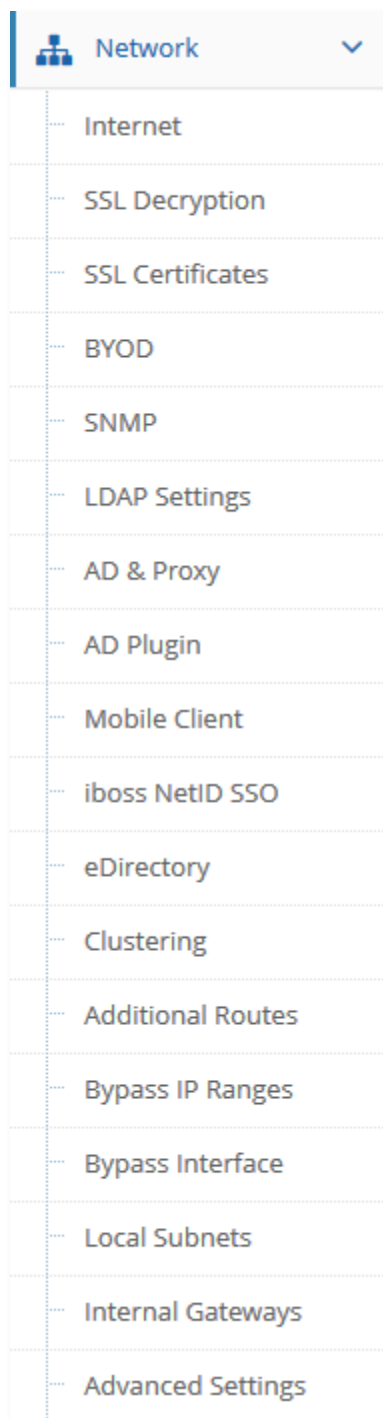


Figure 3 – Network Menu

The "Network" sub-menu lets you choose options for configuring the current iboss connection settings. These are options to choose from: Internet, SSL Decryption, SSL Certificates, BYOD, SNMP, LDAP Settings, AD & Proxy, AD Plugin, Mobile Client, iboss NetID SSO, eDirectory, Clustering, Additional Routes, Bypass Interface, Local Subnets, Internal Gateways, and Advanced Settings.

Internet Connection – This option allows you to configure the Internet WAN connection of the iboss. This page also allows you to configure the device in Tap Mode if you have a management card installed on the device.

Gateway SSL Decryption – This option allows you to enable Gateway SSL Decryption.

SSL Certificate Settings – This option allows you to configure an SSL Certificate to allow https access to the iboss interface to securely access the interface.

BYOD Settings – This option allows you to enable BYOD Authentication settings and custom login page.

SNMP – This option allows you to enable SNMP settings for the device to monitor hardware health of the iboss device.

LDAP Settings – This option allows you to setup your LDAP/Active Directory server so the iboss can authenticate users from it typically used with the Internet Access Window.

Active Directory & Proxy Settings – This option allows you to setup the iboss in a Proxy mode. This will allow automatic Active Directory authentication using NTLM.

Active Directory / Network Access Controller Integration – This option allows you to setup the iboss to work with your Active Directory Server using the iboss Active Directory Plugin. This will allow automatic Active Directory authentication using the plugin on the server. This section also allows you to setup integration with Network Access Controllers for user authentication.

Mobile Client & SSL Inspection Agent – This option allows you to setup the iboss mobile client for Windows, MAC and the iPad/iPod browser. This will allow you to also use the local SSL Inspection Agent.

ibossNetID Single Sign-On Agent – This option allows you to setup the ibossNetID Single Sign-On Agent that installs on the computer as an agent to authenticate usernames for Windows. This section also allows you to setup the Apple Logon Hooks for user authentication with MACs.

eDirectory Settings – This option allows you to setup the iboss with your eDirectory servers for transparent authentication.

Clustering – This option allows you to setup multiple iboss devices in a clustered environment to have settings synced automatically.

Add Additional Routes – This option allows you to add additional network routes for the iboss.

Bypass IP Ranges – This option allows you to bypass IP ranges which you would like to completely bypass the iboss filtering engine.

Local Subnets/IP Ranges – This option allows you to add additional local subnets.

Register Internal Gateways – This option allows you to register gateways that are internal to your network (on the LAN side of the iboss).

Advanced Settings – This option allows you to configure the advanced network settings.

5.1 Configure Internet Connection

Internet Connection

Save

+

Basic Configuration

Inline or Tap

Remote Authentication Integration

Internal Report Manager Listen Port

Status

Ip Address

10.128.16.112

Subnet Mask

255.255.240.0

Default Gateway

10.128.18.1

Primary DNS

8.8.8.8

Secondary DNS

8.8.4.4

MAC Address

68:05:ca:1b:59:75

Figure 4 – Internet Connection

5.1.1 Basic Configuration

Basic Configuration

Connection Type

static

Ip Address *

192.168.1.10

Subnet Mask *

255.255.255.0

Default Gateway *

192.168.1.1

Primary DNS *

192.168.1.1

Secondary DNS *

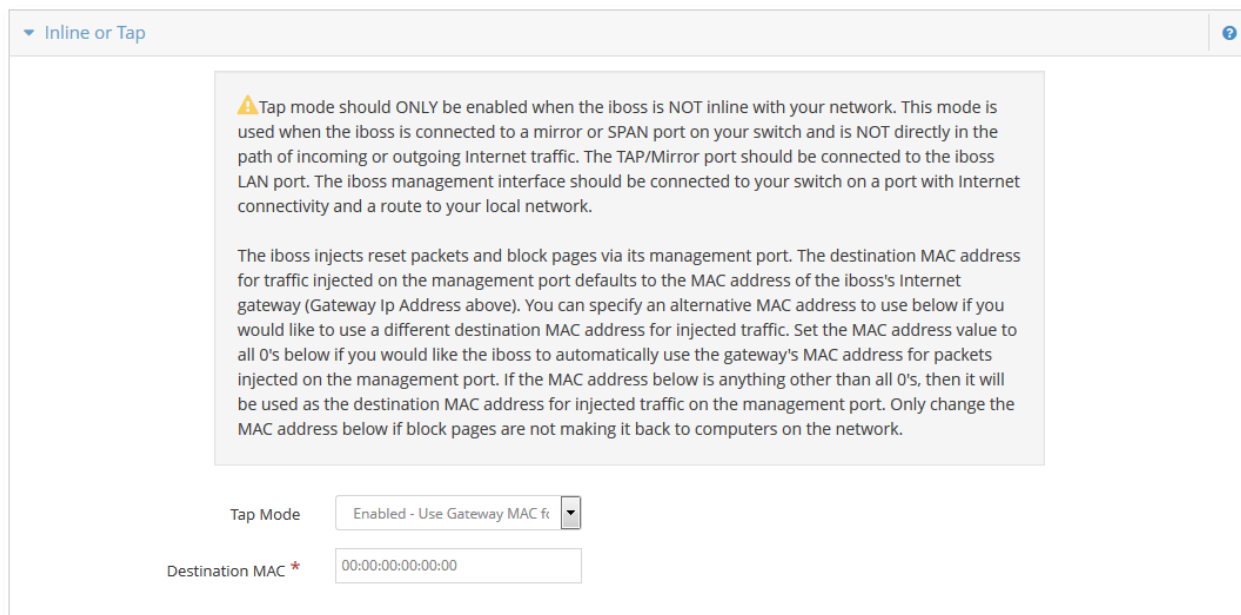
192.168.1.2

Figure 5 – Internet Connection – Basic Configuration

The iboss will need to be configured to have a static IP address.

Manually enter network settings for your WAN connection. These settings should be a unique IP address and match your local network which can be accessible from the management interface of the iboss SWG.

5.1.2 Inline or Tap



▼ Inline or Tap

Warning: Tap mode should ONLY be enabled when the iboss is NOT inline with your network. This mode is used when the iboss is connected to a mirror or SPAN port on your switch and is NOT directly in the path of incoming or outgoing Internet traffic. The TAP/Mirror port should be connected to the iboss LAN port. The iboss management interface should be connected to your switch on a port with Internet connectivity and a route to your local network.

The iboss injects reset packets and block pages via its management port. The destination MAC address for traffic injected on the management port defaults to the MAC address of the iboss's Internet gateway (Gateway Ip Address above). You can specify an alternative MAC address to use below if you would like to use a different destination MAC address for injected traffic. Set the MAC address value to all 0's below if you would like the iboss to automatically use the gateway's MAC address for packets injected on the management port. If the MAC address below is anything other than all 0's, then it will be used as the destination MAC address for injected traffic on the management port. Only change the MAC address below if block pages are not making it back to computers on the network.

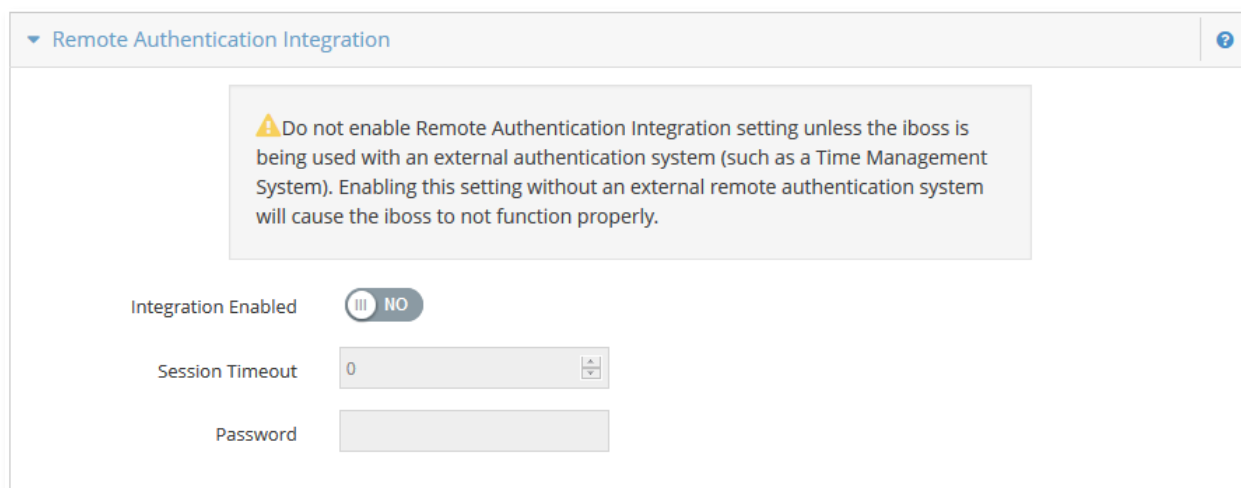
Tap Mode: Enabled - Use Gateway MAC fr

Destination MAC: 00:00:00:00:00:00

Figure 6 – Internet Connection – Inline or Tap

This section allows you to configure the device in a Tap Mode (also known as Mirror or Span Mode). In this mode, you will want to configure where the iboss SWG will inject the block page. Choose one of the options of where to send the block pages.

5.1.3 Remote Authentication Integration



▼ Remote Authentication Integration

Warning: Do not enable Remote Authentication Integration setting unless the iboss is being used with an external authentication system (such as a Time Management System). Enabling this setting without an external remote authentication system will cause the iboss to not function properly.

Integration Enabled: NO

Session Timeout: 0

Password:

Figure 7 – Internet Connection – Remote Authentication Integration

This feature allows Remote Authentication Integration. This is an OEM feature that is only used for third party applications. Typically this is not used unless specifically needed by third party applications.

5.1.4 Internal Report Manager Listen Port

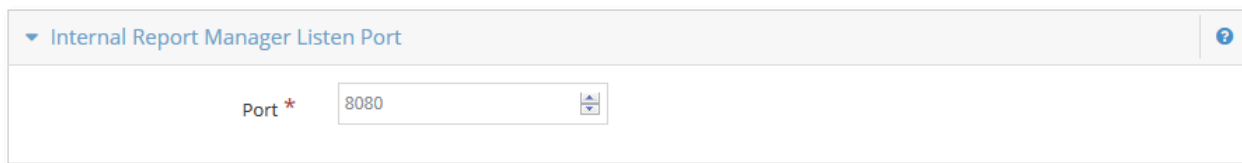


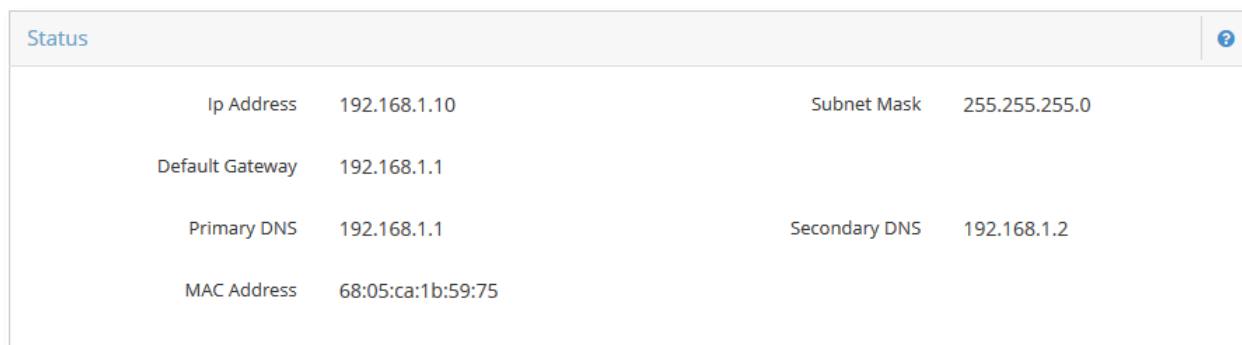
Figure 8 – Internet Connection – Internal Report Manager Listen Port

This section allows you to change the port number that the iboss reports are served from.

Click "**Save**" when you have finished the configuration above. You have completed the WAN configuration for the Static IP Address connection type.

Note: Once the iboss has been configured, you may return your computer's network settings back to their original settings. Also, if the iboss has already been configured to have a different IP Address, you must log into the iboss using these settings. If you do not know what the settings were, you will have to log into the iboss via the serial console port using the instructions described above.

5.1.5 Status



Status			
Ip Address	192.168.1.10	Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1		
Primary DNS	192.168.1.1	Secondary DNS	192.168.1.2
MAC Address	68:05:ca:1b:59:75		

Figure 9 – Internet Connection – Status

This section allows you to view the status of the current IP that is configured for the device.

5.2 Gateway SSL Decryption

5.2.1 Overview

The iboss gateway SSL decryption engine allows the iboss to intercept and decrypt HTTPs/SSL sessions in order to provide content security and controls over encrypted destinations. The iboss decryption goes far beyond traditional HTTPs/SSL decryption solutions by providing unique features and functionality to solve problems associated with performing SSL decryption on HTTPs streams.

The HTTPs/SSL decryption engine provides the ability to perform SSL decryption completely transparently to the endpoint as well as the ability to perform decryption for direct proxy connections. In addition, the engine can be configured to selectively perform decryption on configured destinations vs. performing decryption on all destinations. Decryption can also be performed selectively on particular subnets while not performing decryption on other subnets on the network in order to effectively deal with BYOD on the local network. Users can also be automatically prompted to indicate when an HTTPs/SSL stream is being decrypted to reduce liability, inform the end user of the process in place, as well as provide information on configuring the endpoint to install trusted root certificates in order to avoid browser warnings.

NOTE

SSL Gateway decryption is only available on the iboss series xx60 and xx600. For example, the iboss decryption engine is available on the model iboss 1560 but not the model iboss 1550. Settings are cross compatible and can migrate between the same series. For example, the iboss 1550 settings are compatible with the iboss 1560.

5.2.2 Understanding HTTPs/SSL Decryption

This section provides a general background of how HTTPs/SSL decryption works and provides a general understanding of the related aspects of HTTPs interception and decryption.

5.2.2.1 The HTTPs/SSL Protocol

The HTTPs/SSL protocol is designed to protect communication between a computer and a server. There are two core aspects of HTTPs protocol which provide this protection:

1. **Encryption** – Encryption is used to scramble the data between the computer and the destination server. Scrambled data is designed to make the data unreadable and ideally prevents unintended eavesdropping of the data being sent between the computer and server while the data is being transmitted.
2. **Authentication** – This part of the HTTPs protocol is equally as important as the encryption portion as it provides a method to verify that the destination server the computer is communicating with is really the server the computer thinks it is communicating with. If an intruder were to spoof the server page content, they could easily steal the information transmitted by the computer as the data would be sent to the intruders computer vs. the server that was originally intended to receive the data.

The two aspects of HTTPs/SSL above make it challenging to perform interception of the data in order to inspect and provide security policy. This is because although the gateway inspecting the data is forwarding the data, it cannot see the true content (due to SSL encryption) or pretend to be the destination in order to inspect the data (due to SSL authentication).

In order to perform inspection of the encrypted data, the data must be first decrypted and unscrambled. Ideally the gateway (iboss) should do this as the data traverses the gateway on the way out to the Internet. Performing this function is considered performing a “Man In The Middle” (MITM) interception. This is because the gateway is the man in the middle between the computer and the intended destination. The iboss

intercepts the data, inspects it, and then forwards the data over another encrypted connection to the destination server.

When a man in the middle (MITM) interception occurs, the computer is made aware of this via the built in functionality of HTTPs/SSL. Typically, the user is presented with a screen on their browser indicating the secure connection has been compromised. A few examples of this are show below:

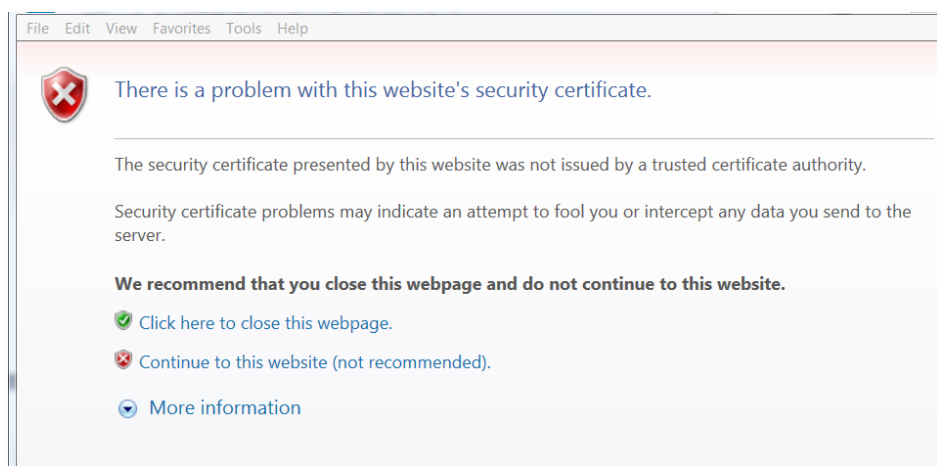


Figure 10 – Internet Explorer Certificate Warning

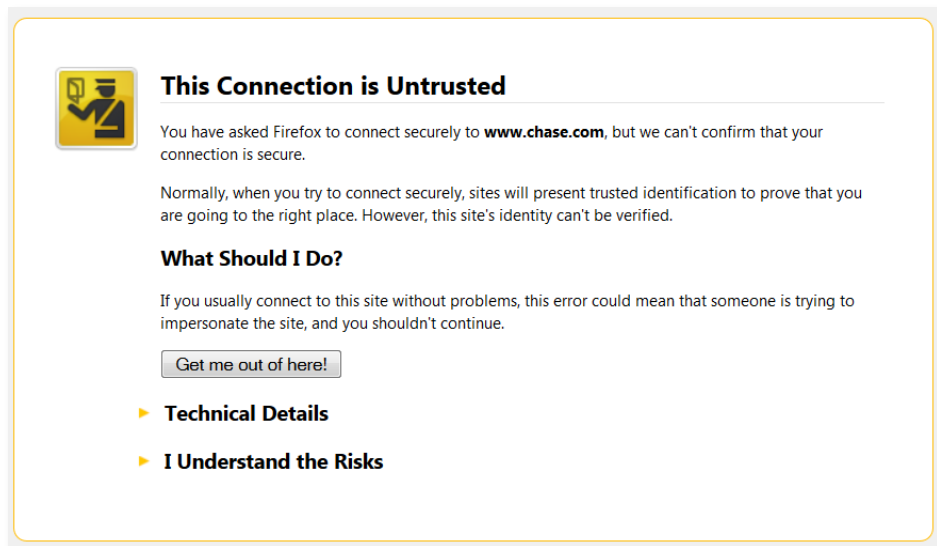


Figure 11 – Firefox Certificate Warning

Although the purpose of the SSL inspection by the gateway may be for legitimate reasons, from the perspective of the browser the SSL session will indicate the SSL interception/decryption has occurred.

The following steps are taken by the iboss decryption engine to perform an SSL interception:

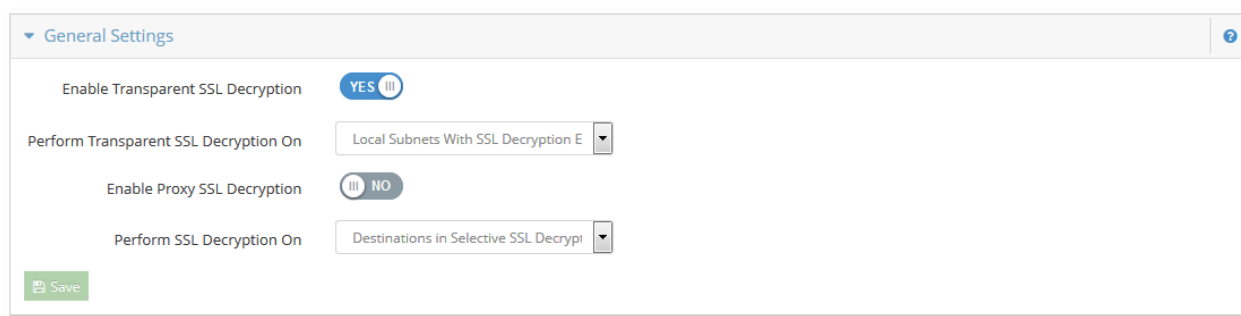
1. Client computer requests SSL site (i.e. <https://www.facebook.com>)
2. iboss intercepts request. iboss then connects to the destination the SSL connection was intended for and fetches the SSL certificate.
3. iboss creates a spoofed SSL certificate and presents it to the client computer based on the original SSL certificate that was sent by the destination server.
4. Client communicates with iboss over the encrypted connection established and forwards requests and responses over the newly established connection between the iboss and the server.

Since the iboss intercepted the request and presented a spoofed certificate, the clients browser will complain with the warning because the certificate presented by the iboss was not issued by a “Trusted Certificate Authority” such as Verisign or Network Solutions. The client computer does not see the iboss as having the ability to generate these types of certificates.

In order to avoid the warning, the client computer can have the root certificate of the iboss installed into the browsers Trusted Certificate Store. Once this is done, the client computer’s browser will no longer complain about an invalid certificate. While this is convenient, it is not required. Without the installation of the iboss root certificate into the browser, the user will continue to get the untrusted connection warning. There are features included with the iboss SSL decryption engine which help alleviate the issues related to the root certificate warning and the installation of the root certificate into the computer’s browser.

It is important to note that the issue regarding invalid certificate warnings applies to any gateway (not just the iboss) that is spoofing an SSL connection and performing a man in the middle decryption. It is due to the fact that this feature is built into the SSL/HTTPs protocol.

5.2.3 General Settings



The screenshot shows the 'General Settings' window for SSL Decryption. It contains four settings:

- Enable Transparent SSL Decryption:** Set to YES (indicated by a blue pill button).
- Perform Transparent SSL Decryption On:** Set to 'Local Subnets With SSL Decryption E' (indicated by a dropdown menu).
- Enable Proxy SSL Decryption:** Set to NO (indicated by a grey pill button).
- Perform SSL Decryption On:** Set to 'Destinations in Selective SSL Decrypt' (indicated by a dropdown menu).

A green 'Save' button is located at the bottom left of the settings panel.

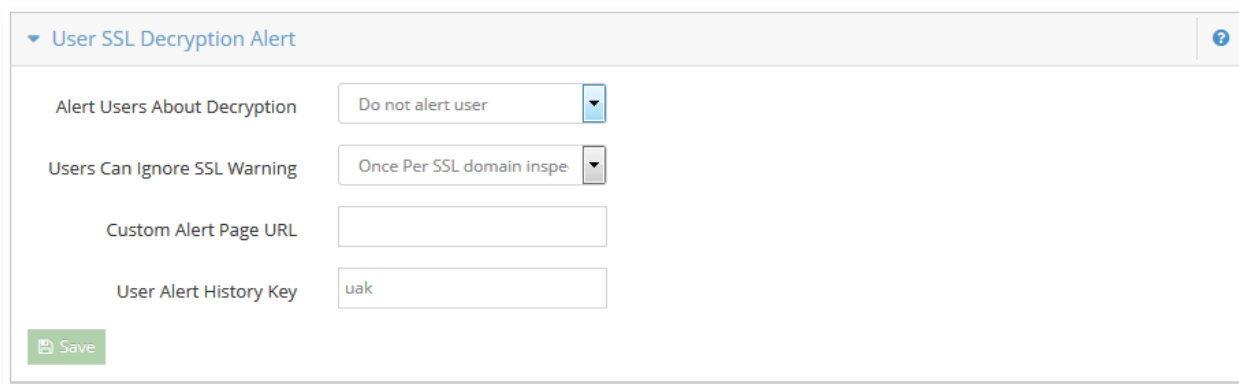
Figure 12 – Gateway SSL Decryption – General Settings

The General Settings section allows you to configure global options which enable and disable the SSL decryption engine. The iboss has the ability to transparently intercept connections and decrypt them without any browser settings. In addition, the iboss can decrypt proxy connections being made to the iboss.

The section below describes the options in the General Settings section:

Enable Transparent SSL Decryption	This option enables transparent SSL interception. When disabled, no transparent SSL interception occurs.
Perform Transparent SSL Decryption On	<p>Options:</p> <p>Local Subnets With SSL Decryption Enabled – This feature allows you to selectively perform SSL decryption for only a select set of local subnets on your network. This feature is great for situations such as BYOD where you may not want to decrypt connections on a wireless BYOD network. Only networks under the “Local Subnets” section with the option “SSL Decryption” set to yes will be transparently intercepted and decrypted.</p> <p>All Local Subnets – This option causes all local subnets to be decrypted regardless of the local subnet’s setting for “SSL Decryption”.</p>
Enable Proxy SSL Decryption	Perform decryption of direct proxy connections accessing SSL sites. This feature is relevant if the proxy is enabled and browsers have proxy settings pointing to the iboss. If this feature is set to “No”, proxy connections accessing SSL sites will not be decrypted.

5.2.4 User SSL Decryption Alert



The screenshot shows a configuration window titled "User SSL Decryption Alert". It contains four settings:

- Alert Users About Decryption:** A dropdown menu currently set to "Do not alert user".
- Users Can Ignore SSL Warning:** A dropdown menu currently set to "Once Per SSL domain inspe".
- Custom Alert Page URL:** An empty text input field.
- User Alert History Key:** A text input field containing the value "uak".

At the bottom left of the window is a green "Save" button with a floppy disk icon.

Figure 13 – Gateway SSL Decryption – User SSL Decryption Alert

This feature allows you to alert users whenever a website they are visiting is going to be decrypted. This feature helps reduce liability as well as inform the user that SSL inspection is taking place for selected domains.

The section relies on the section directly following which allows you to enter a select list of domains into a list. Whenever a user visits a domain in the list from the following section and alerts are enabled, a message will be shown to the user indicating that SSL inspection is taking place as well as provide them with the instructions and download link for installing the root certificate into their browser.

The figure below shows a sample of the message users would see when visiting SSL intercepted domains:

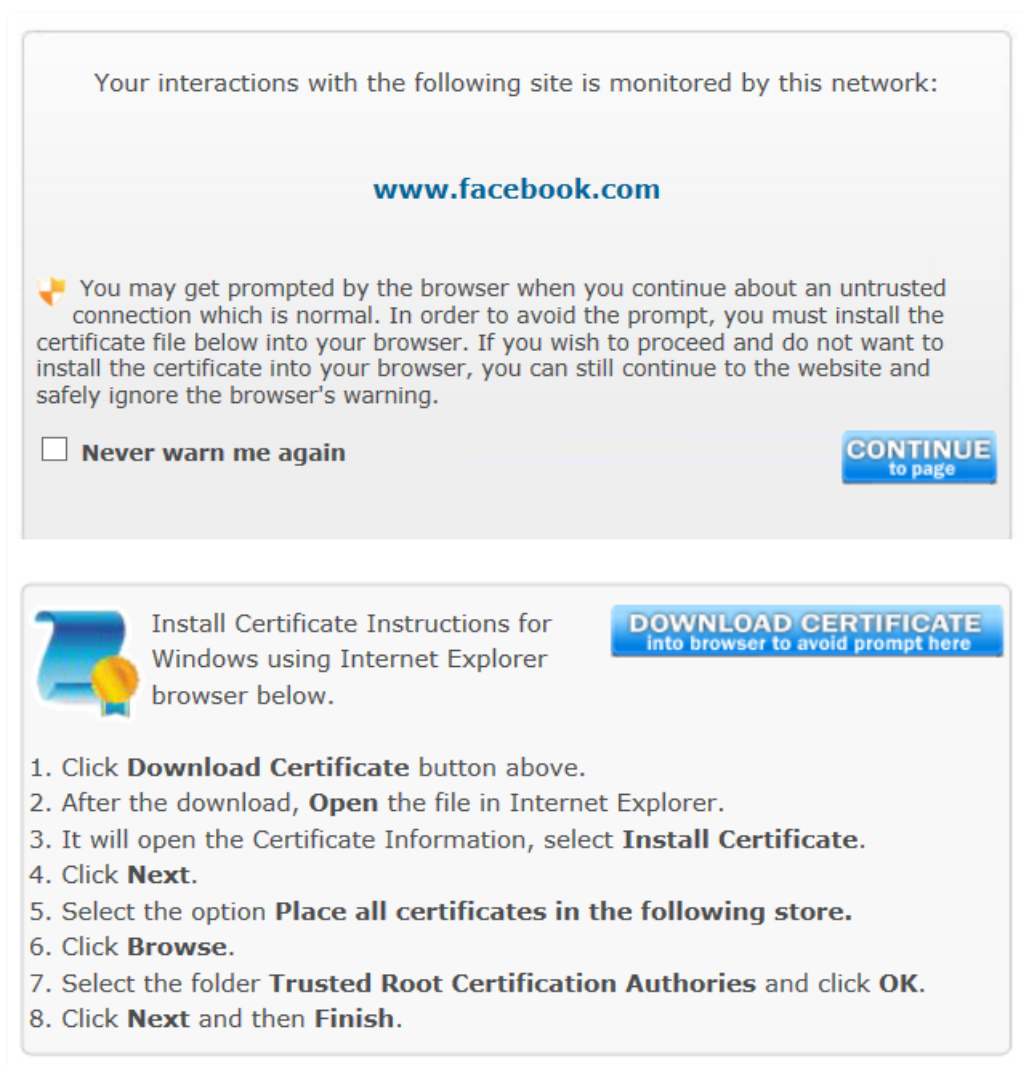


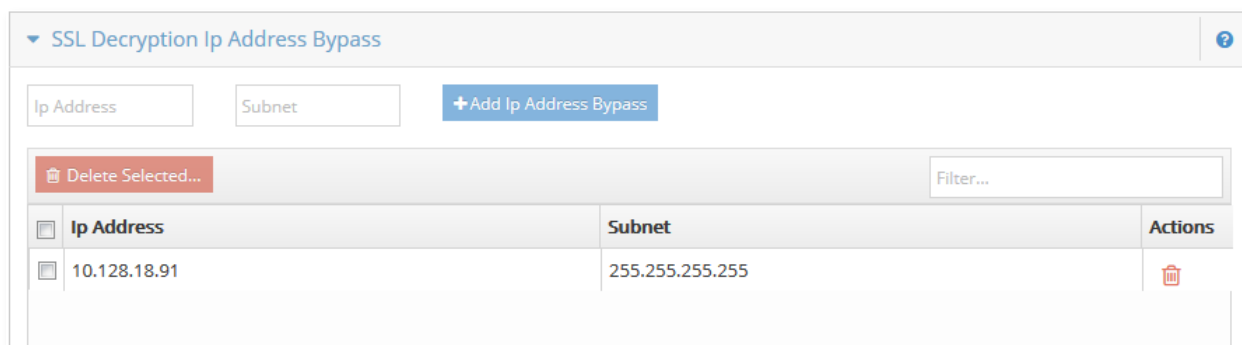
Figure 14 – User Alert When Visiting SSL Intercepted Domain

In the case above, the user visited <http://www.facebook.com> which was a domain that was being SSL intercepted by the iboss. The informative message was presented as well as instructions on installing the root certificate if the user desired to do so.

Alert Users About Decryption	<p>Options:</p> <p><i>On visit to domains below</i> – When this option is selected, visiting domains listed under the section “SELECTIVE SSL DECRYPTION DOMAIN LIST” will cause an informative page to be displayed to the user indicating that SSL inspection is taking place on that domain. Only domains in the list will cause the message to appear. In addition, the message will provide browser specific instructions about how to install the root certificate required to prevent warnings from appearing when the user visits encrypted https pages that are inspected.</p> <p>Do not alert user – No message is displayed to the user when inspection is occurring.</p>
-------------------------------------	---

<p>Users Can Ignore SSL Warning</p>	<p>This option allows the users to check a “Never warn me again” checkbox so that the alert no longer appears when visiting the intercepted SSL domain. The options are:</p> <p>Once per SSL domain inspected – If the user checks the never warn again checkbox, the warning is no longer shown for the specific domain the user was visiting. The warning will appear on other domains being SSL intercepted. This option is good when you would like to warn users at least once per domain that SSL interception is occurring.</p> <p>Once for all SSL domains inspected – If the user checks the never warn again checkbox, the warning does not appear on any other SSL intercepted domain.</p> <p>No, users cannot ignore warning – Users do not have the option to check the “Never warn me again” checkbox effectively causing the warning to show up whenever an SSL inspected domain is visited.</p>
<p>Custom Alert Page URL</p>	<p>This allows you to customize the alert page by hosting the alert page on a separate server. Enter the full URL to the external warning page. It is a good idea to copy the source of the built-in warning page to use as a template when creating your custom warning page.</p>
<p>User Alert History Key</p>	<p>This is a unique key that is used to store the “Never warn me again” option into the user’s browser. If you would like to re-prompt all users again (due to a changed warning page for example), simply change this value to any other random value and all users will automatically be re-warned. The default value is “uak”. So to change the value, simply append a digit to the end (for example, uak2) whenever you want to re-prompt all users.</p>

5.2.5 SSL Decryption IP Address Bypass



Ip Address	Subnet	Actions
10.128.18.91	255.255.255.255	

Figure 15 – Gateway SSL Decryption – SSL Decryption IP Address Bypass

This section allows you to fully bypass transparent SSL interception and decryption for any IP Address or subnet. This includes both local and non-local IP Address sources and destinations.

Enter IP Addresses you wish to fully bypass and hit the Add button. To remove an item from the list, select the box next to the IP Address and hit the “Remove Selected IP Addresses” button.

5.2.6 Selective SSL Decryption



Domain	Actions
facebook.com	
skype.com	

Figure 16 – Gateway SSL Decryption – Selective SSL Decryption

The selective SSL decryption section is a unique feature of the iboss that allows you to selectively intercept only a select set of domains. This feature is powerful in that it allows you to pick only those domains which you would like to inspect and decrypt only those destinations. For other SSL destinations, the encrypted SSL stream is left untouched. For example, if you wanted to only inspect <https://www.facebook.com> for social media controls but not <https://www.chase.com>, you could enter facebook.com into the list which would cause only that domain to be intercepted. This is also great for avoiding unnecessary prompts to sites which you have no desire to decrypt.

To enable selective SSL decryption, configure the following option in this section:

Perform SSL Decryption On	Options:
----------------------------------	-----------------

	<p>The domains listed below – Decryption will only occur on domains in the selective decryption list.</p> <p>All destinations – Decryption occurs on all destinations</p>
--	--

When the option is set to "The domains listed below", selective SSL decryption is enabled.

From the figure above, only facebook.com and skype.com will be decrypted.

NOTE	<p>In almost all cases, always add the www. prefix of the domain to the list. For example, both facebook.com and www.facebook.com are added in the list above. This allows more fine-tuned control in case the www. prefix domain does not resolve to the same website and you do not wish to decrypt it. In that case, you can add the base domain without the adding the www. version of the domain.</p>
-------------	--

5.2.7 Additional SSL Decryption DNS Servers

The screenshot displays a web interface for managing DNS servers. At the top, there's a header 'Additional SSL Decryption DNS Servers' with a help icon. Below it, a text input field for 'Ip Address' is next to a blue button labeled '+ Add Additional DNS Server'. A table below contains one row with the IP '8.8.4.4'. To the left of the table is a red button 'Delete Selected...' and to the right is a 'Filter...' search box. The table has columns for 'Ip Address' and 'Actions'.

Figure 17 – Gateway SSL Decryption – Additional SSL Decryption DNS Servers

This is a specialized section that allows you to add your local DNS servers so that the domains listed under the selective SSL decryption section can be resolved more quickly.

NOTE	<p>Adding your local DNS servers to this section is not required. You should add them if you are finding the delays are too long between changing the selective DNS decryption list and the settings taking affect.</p>
-------------	---

Whenever a selective SSL decryption domain is added, the DNS servers of the iboss network settings are queried to resolve those server's IP addresses in addition to using other resolution algorithms. Adding additional servers to the list causes the DNS servers in the list to be queried as well as the iboss network settings DNS servers when resolving the selective SSL domains to their respective IP addresses.

5.2.8 Conclusion

The advanced algorithms provided by the iboss gateway SSL decryption engine allow you to intelligently inspect SSL encrypted content to sites using the HTTPs/SSL protocol to protect the transaction. The settings provide a scalable, flexible and fluid method to deploy SSL inspection across your enterprise.

5.3 SSL Certificate Settings

SSL Settings

Actions Save

This page allows you to configure the SSL certificates used by the iboss.

SSL Certificate (PEM)

```
-----BEGIN CERTIFICATE-----
MIIC2TCCAjYCCOD/e2gCi5mYmTANBgkqhkiG9w0BAQUFADCBqjELMAkGA1UEBhMC
VVMxEzARBgNVBAGTCkNhbGlmb3JuaWEuEjAQBgNVBAcTCVNBhbiBEaWVnbzEfMB0G
A1UEChMWaWJvc3MgTmV0d29yayBTZWN1cmI0eTEZMBcGA1UECzMqTmV0d29yayBT
-----END CERTIFICATE-----
```

SSL Key (PEM)

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDMK1HnQdcGLnsjykbjbV7PpkU384GIMQb6Zs+k+hQyQavxdPi
biQDH5oknhuDFEBxrq6ibNCL3+64oQTbvLqDdX9mJEk3IWBrdFbneV3onBK4Gubc
XsizrGjuDc9Jai2Ki71GjEhMzVYIJN59yt0OsbX87yAsFV2jCmL9dFWWmQIDAQAB
-----END RSA PRIVATE KEY-----
```

SSL CA (PEM)

```
-----BEGIN CERTIFICATE-----
MIID2jCCA0QgAwIBAgIJAP3gn2vW7FRVMA0GCSqGSIb3DQEBBQUAMIGIMQswCQYD
VQQGEWJlUzETMBEGA1UECBMqQ2FsaWZvcmlpYTESMBAGA1UEBxMJU2FuIERpZWdv
MR0wGAYDVQQKEExFpQm9zcjBxZWlglRmlsdGVycyZEMBCGA1UECzMqTmV0d29yayBT
ZWN1cmI0eTEUMBIGA1UEAxiMLbXlpYm9zcj5jb20xIDAeBgkqhkiG9w0BCQEWEXN1
-----END CERTIFICATE-----
```

Figure 18 – SSL Settings

This page allows you to configure SSL settings used for accessing the iboss interface securely. There is an SSL certificate in there by default to use but you can create your own SSL certificate to access the iboss via https.

Actions allow you to download the current certificate install on the device.

5.4 BYOD Settings

BYOD Settings

General Settings

Enable BYOD Web Login

YES III

User Inactivity Timeout

0

Custom Mobile Login Page

Use Encryption On Mobile Login

YES III

Save

Figure 19 – BYOD Settings

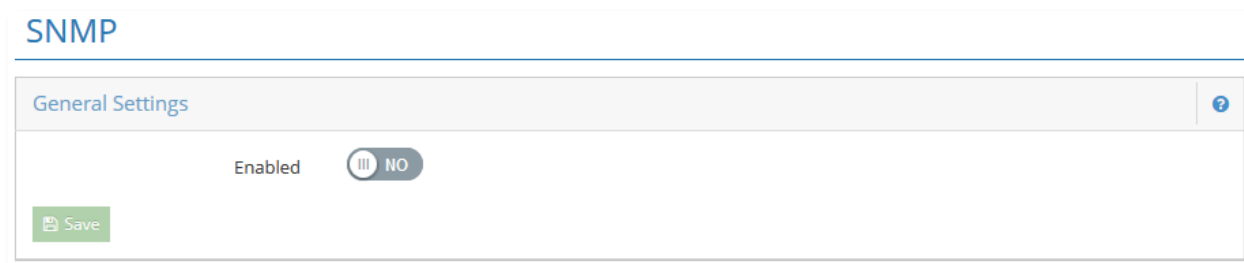
Enable BYOD Web Login – Enables the different login features for BYOD devices such as Android phones. This login does not require an open window to maintain the login, and features a customizable timeout to allow for longer sessions.

User Inactivity Timeout – Determines how long a stale user session for this login stays active before requiring re-authentication. If set to '0', the session remains open indefinitely.

Custom Mobile Login Page – If set, the URL of the login page set here will be used for BYOD devices. This allows for different login page types.

Mobile Login Use Encryption – If set to no, encryption will not be enabled on the login, and it will use the filter's IP address for the login. If set to yes, the connection will be encrypted and the FQDN of the filter will be used. (Ex. Iboss.myiboss.com) This is necessary if these settings will be used for proxy connections outside the network.

5.5 SNMP Settings



The screenshot shows a web interface for SNMP settings. At the top, the title 'SNMP' is displayed in blue. Below it is a 'General Settings' section with a light gray background. Inside this section, there is a toggle switch that is currently set to 'NO', with the word 'Enabled' to its left. A green 'Save' button is located at the bottom left of the settings area. A small blue question mark icon is visible on the right side of the 'General Settings' header.

Figure 6 – SNMP Settings

This section is only available on models 4550 and above. It allows for querying by an SNMP server.

5.6 LDAP Settings

LDAP Settings

Global Settings

Number of LDAP Processors * 25

Max LDAP Retries * 12

LDAP Retry Interval * 10

Max Queue Size * 3000

Tokenize Groups ☒ YES ☐ NO

LDAP Retry Count 0

Save

LDAP Servers

Delete Selected... + Add LDAP Server ...

Filter...

	Name	Server Hos...	Port	Server Type	Match Gro...	Match Gro...	User Searc...	Search Base	Actions
<input type="checkbox"/>	testad2	10.128.16.16	389	General LD...	memberOf	CN	(sAMAccou...	dc=yourdom...	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	SCHOOL2	22.22.22.22	389	General LD...	memberOf	CN	(sAMAccou...	dc=yourdom...	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Figure 20 – LDAP Settings

5.6.1 Global Settings

This section allows you to set global LDAP settings.

Number of LDAP Processors – This is how many LDAP processors are used within the iboss for authentication. 25 is the default.

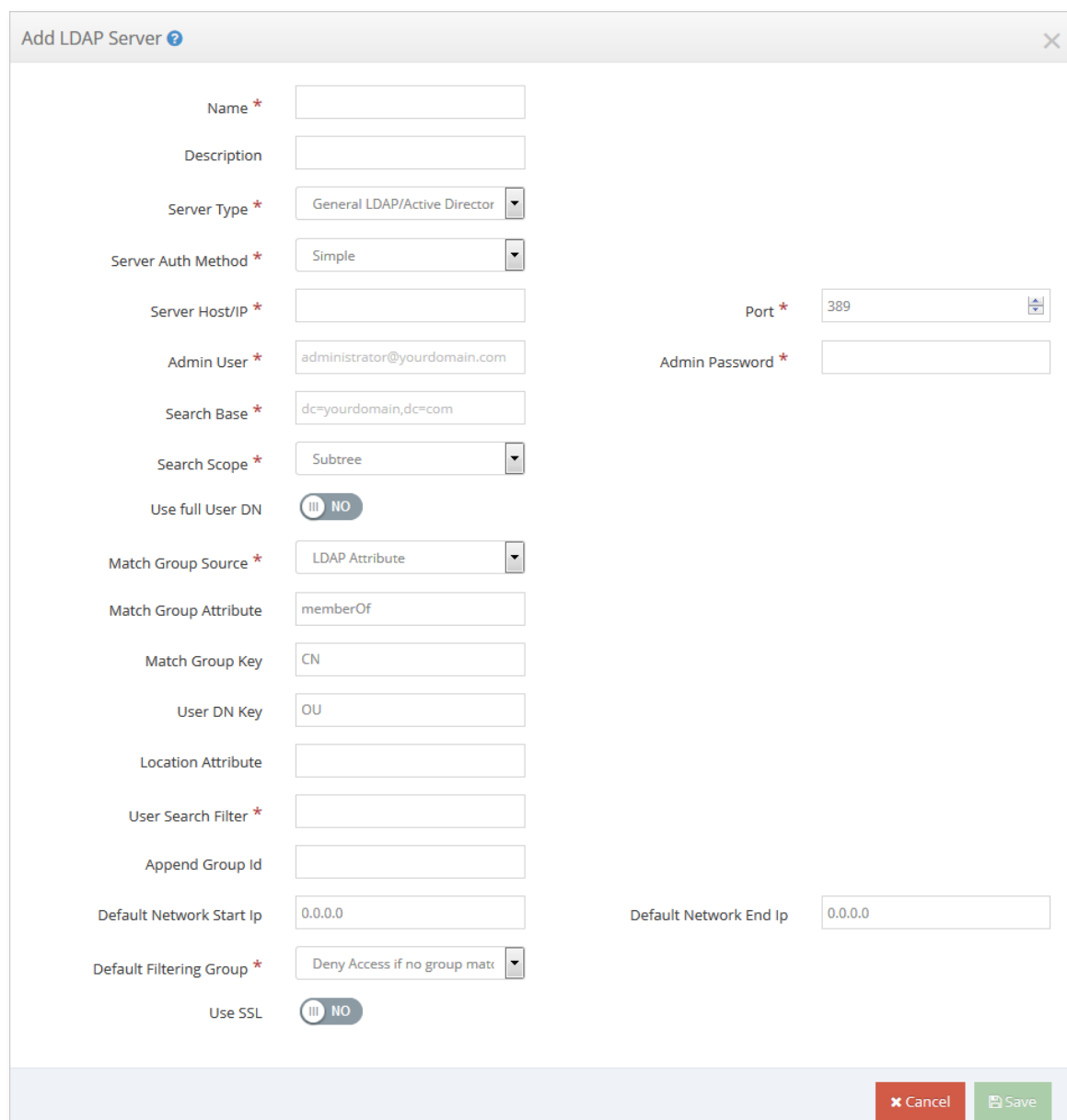
Max LDAP Retries – This is the number of retries before the authentication is no longer tried. 12 is default.

LDAP Retry Interval – This is the interval between retries if authentication is not successful. 10 Seconds is the default.

Max Retry Queue Size – This is the max number of queue spots for LDAP authentication retries.

Tokenize Groups – This option allows you to tokenize group names per word in a group. For example, Staff can be parsed out of a group named Location 1 Staff.

5.6.2 Add LDAP Server



The 'Add LDAP Server' dialog box contains the following fields and controls:

- Name ***: Text input field.
- Description**: Text input field.
- Server Type ***: Dropdown menu with 'General LDAP/Active Director' selected.
- Server Auth Method ***: Dropdown menu with 'Simple' selected.
- Server Host/IP ***: Text input field.
- Port ***: Spin box with '389' selected.
- Admin User ***: Text input field with 'administrator@yourdomain.com'.
- Admin Password ***: Password input field.
- Search Base ***: Text input field with 'dc=yourdomain,dc=com'.
- Search Scope ***: Dropdown menu with 'Subtree' selected.
- Use full User DN**: Radio button group with 'NO' selected.
- Match Group Source ***: Dropdown menu with 'LDAP Attribute' selected.
- Match Group Attribute**: Text input field with 'memberOf'.
- Match Group Key**: Text input field with 'CN'.
- User DN Key**: Text input field with 'OU'.
- Location Attribute**: Text input field.
- User Search Filter ***: Text input field.
- Append Group Id**: Text input field.
- Default Network Start Ip**: Text input field with '0.0.0.0'.
- Default Network End Ip**: Text input field with '0.0.0.0'.
- Default Filtering Group ***: Dropdown menu with 'Deny Access if no group mat' selected.
- Use SSL**: Radio button group with 'NO' selected.

At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 21 – LDAP Settings – Add LDAP Server

Name – This is the name of the server to assist in identification.

Description – This option allows you to set a description for the server that is being added.

Server Type – This option allows you change the server type from General LDAP/Active Directory to Open Directory and Open LDAP.

Server Authentication Method – This option allows you to configure the server authentication method required by your LDAP server. Simple is recommended.

Server Host/IP – This is the domain or IP address of the LDAP server. Example: iboss.com or 10.0.0.1

Port – This allows you to change the port number that is used to communicate to your LDAP server. Port 389 is most common and is recommended.

Admin User – This is the Username of an administrative or root user which has administrative rights to your LDAP server. The user must be able to perform searches on your LDAP server. This user is used to look up user logins. Example: administrator@iboss.com.

Admin Password – This is the password to your LDAP administrator user above. Some special characters are not accepted.

Search Base – This is the base by which searches for users will be made. If you have a large directory you may choose a base other than the top as long as all users that need to be authenticated are under this base. It is recommended that you set this to the top of your LDAP directory. Example: If your LDAP domain is iboss.com, you would use the following settings: dc=iboss,dc=com

Search Scope – This allows you to configure whether you would like to search only the selected level or everything beneath it (sub tree).

Match Group source – You may select to look for group matches within an LDAP attribute specified by 'Match Group Attribute' or the 'User DN' or both.

Match Group Attribute – This is the attribute within the user record to search for groups. The group names are matched to the iboss filtering groups. The group names must match exactly.

Match Group Key – If a filtering group attribute is found and contains many key value pairs, you can limit the group match to a particular key. For example, if a group value contains 'CN=managers,OU=support' you may choose to match groups to the 'CN' key which would match the word 'managers' to the iboss filtering group. If you leave this field blank, the entire group attribute will be used. Active Directory Example: CN

User DN Key – If 'User DN' is included within the 'Match Group Source' option then this key is used to parse the User DN. Active Directory Example: OU

Location Attribute – Deprecated

User Search Filter – This is the filter that is used to search for a username in the LDAP server. This filter must result in a single user record. The filter must also contain %s which will be replaced by the username. There must not be any other percent signs in the search filter. Active Directory Example: (sAMAccountName=%s)

Active Directory Overview: An LDAP query is made for the sAMAccountName attribute containing the username and thememberOf attribute is requested. The value of thememberOf attribute will be the DN of each group that the user belongs to. The Group Key of CN is used to search the returned DN values for the group names. These names are compared to your iboss filtering groups. If there is a match that filtering group is used. If there are multiple matches, the filtering group configured with the highest priority is used.

Append Group ID – This option allows you to append a group ID to each group name or OU that the user belongs to allowing overlapping group names from different LDAP domains.

Default Network Start IP/End IP – This option will apply LDAP lookups for computers that fall in this network range.

Default Filtering Group – This option allows you to use a default filtering group if no LDAP group can be matched with an active iboss Filtering Group. You can choose to Deny Access if no group match or choose between the different filtering groups.

Use SSL – This option allows you to turn on SSL encryption with your LDAP server

Once you have finished entering information, click the **Save** button. Once it has been added, click the **Test** button (the checkmark icon) next to the entry in the box. If you would like to edit the server information, click the **Edit** button (the pencil icon) and the fields will be able to edit. Once updated, click the **Save** button.

5.6.2.1 Match Active Directory Groups with iboss Filtering Groups

Once you have the LDAP/Active Directory Settings configured, you will need to match your Active Directory groups with the iboss filtering groups. You can simply rename the filtering group names to match the Active Directory group names. To do this, from the main menu click on Groups. If a user belongs to multiple groups, the user will fall under the highest priority filtering group number. Please refer to Filtering Groups section for more details.

5.7 Active Directory & Proxy Settings

Active Directory & Proxy Settings

Actions
Save

Settings

Enable Proxy Settings
YES

NTLM Authentication Port *
8008

Filtering Method *
Transparent Auto-Login (Dn

User Authentication Method *
Use local iboss User Creden

Unidentified User Group Action *
Use Default Filtering Group

Default Landing Page
http://www.google.com

Proxy Port *
8009

Default Filtering Group *
Group 1

Proxy Cache Settings

URL to Purge from C
Purge URL from Cache

Proxy Cache Size
2000

Max Cache Object Size
4096

Max Cache Object Size Held In Memory

Reserved Cache Memory
256

Cache Memory Pool Size
128

Cache Max File Descriptors
65535

Bypass Cache URL List

Figure 22 – Active Directory & Proxy Settings

5.7.1 Settings

By default, the iboss works as an inline filter that actively scans Internet streams to and from the Internet. This allows the iboss to scan web requests and Web 2.0 application streams. In this mode, each computer is typically named after the primary user of the computer. In the reports, the username will represent the computer.

Alternatively, the iboss can be configured to work as a proxy. This mode is typical of most other filters. In this mode, computers make requests to the iboss at which point the request is made by the iboss on their behalf with filtering applied. This requires that proxy settings be placed in the browser through an Active Directory Group Policy Object or manually. In this mode, the proxy will analyze web requests. For applications to be

analyzed, the iboss must be placed inline on the network so that the iboss can see the streams. For Web 2.0 streams, the policy for that computer will be applied instead of the proxy user.

If using the iboss in an Active Directory environment, NTLM can be used to transparently log the user onto the proxy using the Active Directory credentials. This will apply to all web requests. The iboss can still be used in proxy mode in environments that do not use Active Directory. In this case, users will need to be created within the iboss and the user will be prompted the first time they open a browser for their credentials.

To use the iboss as a proxy filter, you will need to configure the settings for it. You may configure the settings by going to Configure Proxy Settings under the Setup Network Connections section. You will first need to enable this feature. You may change the port number that it uses (by default it uses port 8008). You may then select which User Authentication Method to use. If you have an Active Directory server, you may select Active Directory (NTLM). If you do not have an Active Directory server, you may still use the iboss in Proxy mode and authenticate using the iboss users. Enter all the information for the remaining fields like username and password for your active directory, etc. Please see the examples and help link for further details.

Enable Active Directory & Proxy Support – This option allows you to enable or disable Active Directory & Proxy Support. To use the iboss as a proxy filter or NTLM transparent authentication with Active Directory, you will need to enable this option.

NTLM Authentication Port – This option allows you to configure the NTLM Port that the iboss uses to authenticate users.

Proxy Port – This option allows you to configure the port number to use as a proxy port for the users' browser settings.

Filtering Method – The iboss can be configured in Proxy Mode or Transparent Auto–Login Filtering Mode. In Proxy Mode, the clients' browsers must be configured to use the iboss as a Proxy. This mode is useful if you do not intend to use the iboss inline on your network.

In Transparent Auto–Login Filtering Mode, the iboss performs filtering transparently. This is the default operation of the iboss. However, when this mode is enabled and coupled with NTLM, the iboss will automatically authenticate users via Active Directory. See Help for the differences between 'IP Mode' and 'DNS Mode', which allows you to change the filtering method.

The options are **Proxy Mode, Transparent Auto–Login (DNS Mode), Transparent Auto–Login (IP Mode), Proxy Only (No Filtering)**.

User Authentication Method – This option allows you to configure whether to authenticate using **Active Directory (NTLM), Local iboss User Credentials, Active Computer Policy** or **Mobile Devices (Source IP Address Based)**.

NOTE

When NTLM is selected, the DNS IP Address settings of the iboss must be set to your Active Directory IP Address.

Unidentified User Group Action – This option allows you to change the action used when an unidentified user is found. You can either choose to block access or use a filtering group.

Default Filtering Group – This option allows you to choose the filtering group that is used when an unidentified user is found.

Default Landing URL – This option allows you to specify where the page is redirected after a successful authentication. This is only the case where NTLM was done without an original destination page was first requested.

Admin Username (Only in Active Directory (NTLM) Authentication Method)

– This is the username of the LDAP administrator. Ex: Administrator.

Admin Password (Only in Active Directory (NTLM) Authentication Method)

– This is the password of the administrator user above for your LDAP/Active Directory server.

Domain Name (Only in Active Directory (NTLM) Authentication Method)

– This is your Active Directory domain. Ex: ibosstech.local

Domain IP (Only in Active Directory (NTLM) Authentication Method)

– This is the Domain IP address of your Domain Controller (Active Directory server)

Domain NetBIOS Name (Only in Active Directory (NTLM) Authentication Method)

– This is the name of your workgroup or Domain NetBIOS name. This is what shows up in the drop down menu when users log in. Ex: ibosstech

Active Directory Search Base (Only in Active Directory (NTLM) Authentication Method)

– This is the search base of your Active Directory server. Ex: dc=ibosstech,dc=local

Location Attribute (Only in Active Directory (NTLM) Authentication Method)

– This is the location Attribute within Active Directory if you have multiple locations.

WINS Server IP Address (Only in Active Directory (NTLM) Authentication Method)

– This is the WINS Server IP Address which is commonly the IP address of your Active Directory server.

Password Server IP Address (Only in Active Directory (NTLM) Authentication Method)

– This is the Password Server IP Address which is commonly the IP address of your Active Directory server.

Number of Authenticators – This is the number of NTLM authenticators that try to do authentication.

Authentication Retry Seconds – This option allows you to configure how long to retry authentication in seconds. 0 = disabled.

Active Directory Logon/Logoff Scripts – When NTLM is selected, use the following logon/logoff scripts to add to the Group Policy Object (GPO) on your Active Directory server where your users log in. There are two logon scripts and one logoff script. Place the two logon scripts into the logon scripts folder on your Active Directory GPO. Place the logoff script on the logoff scripts folder on your Active Directory GPO. When registering the logon scripts, only register the primary logon script below. The secondary logon script only needs to be placed in the logon scripts folder on the GPO and should not be registered as a logon script as it only needs to be accessible by users on the network.

You can then download the Primary Logon Script, Secondary Logon Script, and Logoff Script. These scripts can be added to your Active Directory Group Policy to transparently authenticate when users log in.

After entering the information, click '**Save**' and then '**Test**'.

5.7.2 Proxy Cache Settings

Purge URL From Cache – This button allows you to purge individual URLs from the Proxy cache.

Proxy Cache Size – This option allows you to set the Proxy Cache Size. The default is 1000 MB.

Max Cache Object Size – This option allows you to set the Max Cache Object Size. The default is 4096 KB.

Max Cache Object Size Held In Memory – This option allows you to configure the Max Cache object size held in memory. The default is 8 KB.

Reserved Cache Memory – This option allows you to set the Reserved Cache Memory. The default is 256 MB

Cache Memory Pooling Size – This option allows you to set the Pooling Size. The default is 16 MB.

Cache Max File Descriptors – This option allows you to set the Cache Max File Descriptors. 1024 is the default.

Cache Info – This shows the size of the Cache. You can choose to [Purge Cache](#) or [More information](#) about the proxy (see screenshot below for proxy information).

Bypass Cache URL List – This option allows you to bypass URLs in the proxy.

5.7.2.1 Proxy Mobile Devices (Source IP)

Mobile Devices (Source IP Based) option under User Authentication Method on the AD & Proxy settings page is an authentication method that allows the proxy to authenticate users based on their source IP. When a new client hits the proxy and this authentication method is enabled, the client is redirected to an https page where they can enter their credentials (local or LDAP). Once the user authenticates, the username is associated with that source IP and the user can surf through the proxy (logs are associated with username).

Now, if the client is mobile, the source IP is still added to the computers list and marked **(Mobile)**. This allows this method to be used for mobile filtering (especially in cases where they are not using MDM or are using Apple Configurator or something other than MobileEther).

The new feature works by programming the device with a Pac script which is hosted on the iboss (link shown on proxy page authentication drop down list) or downloaded and placed on external webserver if additional proxy Pac configuration is necessary.

The address is based on the hostname and domain that is setup for the iboss under Home → Preferences → System Settings.

Example Proxy Pac code

```
function FindProxyForURL(url,host) { if(localHostOrDomainIs(host,"iboss-lab.phantomtech.local")) {return "DIRECT"; } else{ return "PROXY iboss-lab.phantomtech.local:8009"; } }
```

5.7.2.2 Automatic GPO Setup for NTLM with Logon/Logoff Scripts

Add the Logon and Logoff scripts to the Active Directory as a group policy when users log in and log off for NTLM Authentication. To do this, follow these steps:

1. From within your Active Directory server, go to Start → Programs → Administrative Tools and click on 'Active Directory Users and Computers'
2. Right-click on the domain and select Properties, then select the Group Policy tab.
3. Select the 'Default Domain Policy' and click Edit.
4. Navigate to User Configuration → Windows Settings → Scripts (Logon/Logoff)
5. Double click Logon and click Show Files, move the login files here.
6. Next click add and select the primary logon script
7. Do the same for the Logoff script.
- 8.

5.7.2.2.1 Automatic GPO Setup for NTLM with Internet Explorer

The automatic GPO Setup for NTLM will allow your Active Directory server to setup and distribute the Proxy Settings within the domain clients' Internet Explorer browser for you. To do this, follow these steps:

1. From within your Active Directory server, go to Start → Programs → Administrative Tools and click on 'Active Directory Users and Computers'
2. Right-click on the domain and select Properties, then select the Group Policy tab.
3. Select the 'Default Domain Policy' and click Edit.

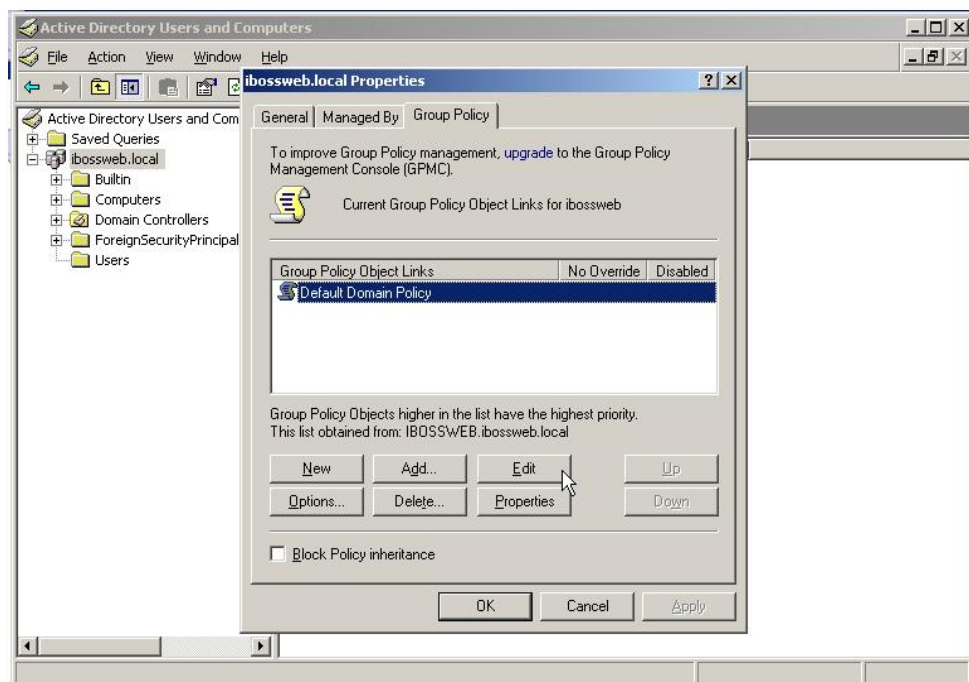


Figure 23 – GPO Default Domain Policy

4. Navigate to User Configuration → Windows Settings → Internet Explorer Maintenance → Connection
5. Double-click on Connection Settings in the right window panel.

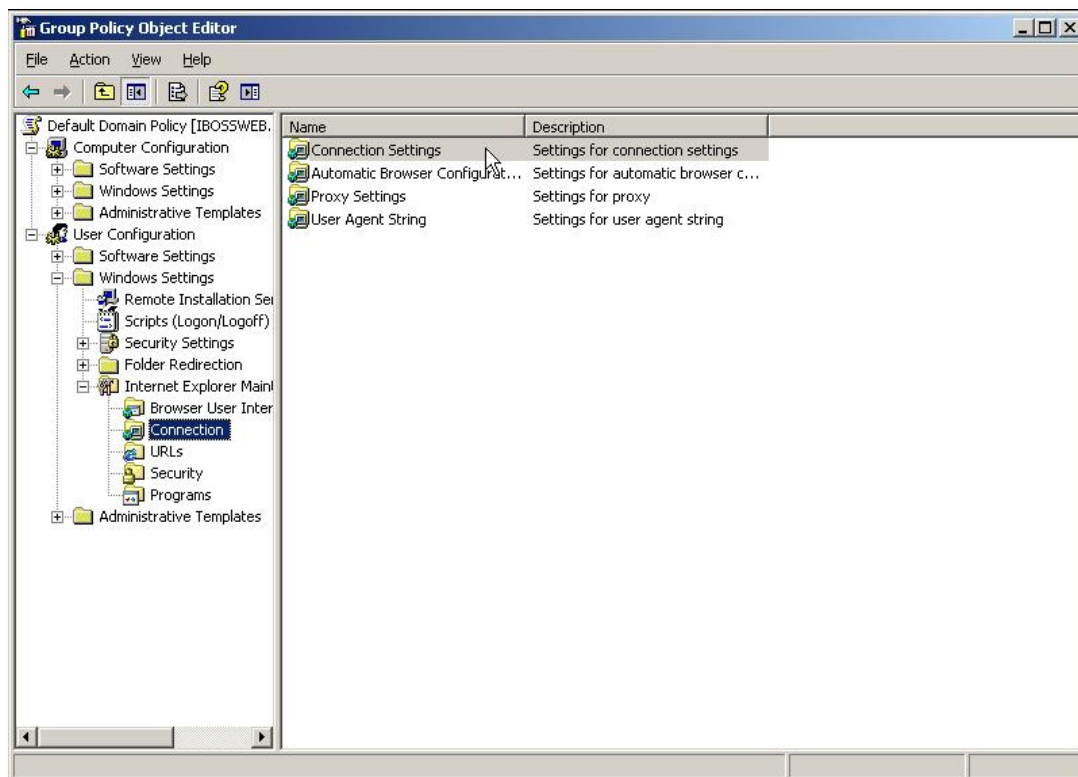


Figure 24 – GPO Connection Settings

6. Select the option 'Import the Connection Settings' and click Modify Settings.

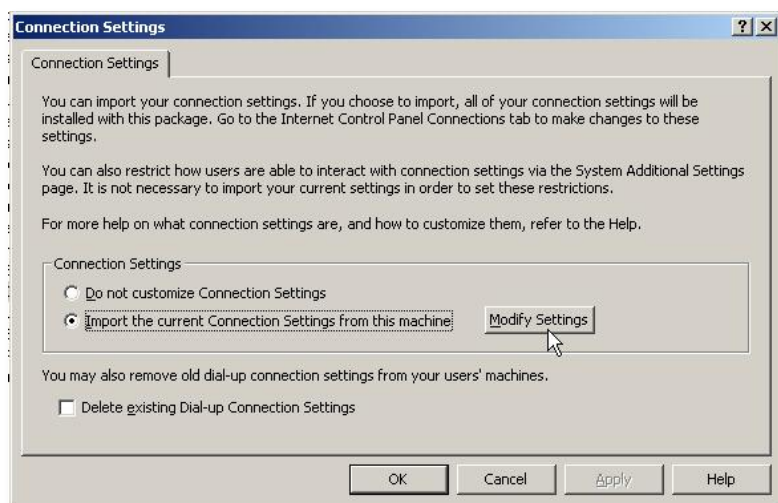


Figure 25 – GPO Import the Connection Settings

7. Click 'LAN Settings' and check 'Use a proxy server'.

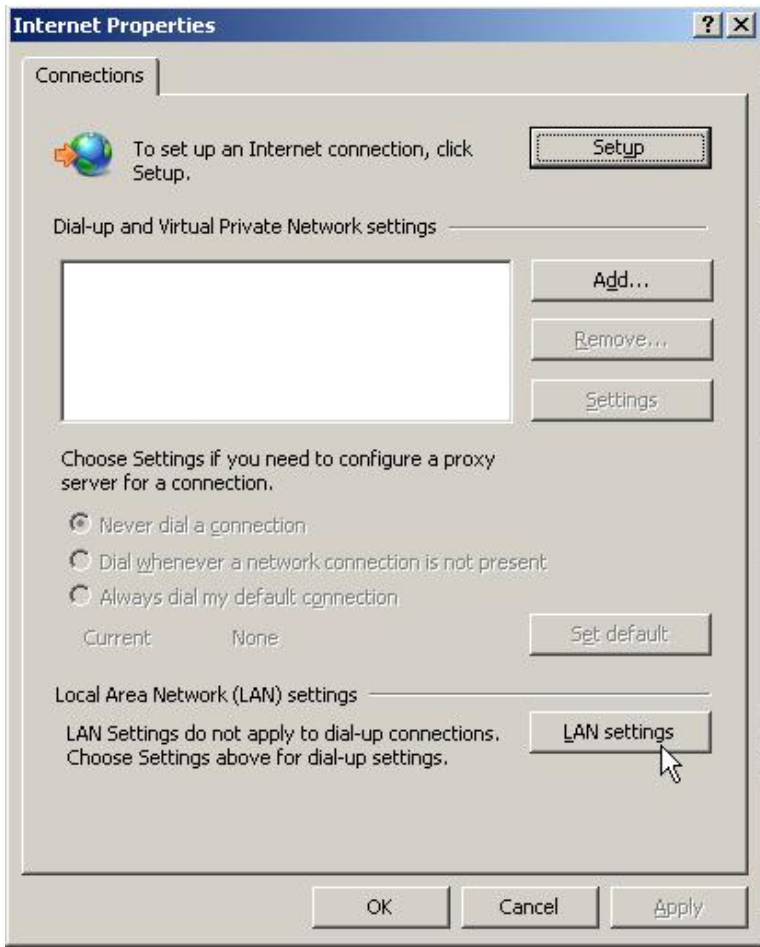


Figure 26 – GPO Use Proxy Server

8. Enter the IP address of the iboss and the Proxy port that is setup on the iboss (default 8008) and click OK.

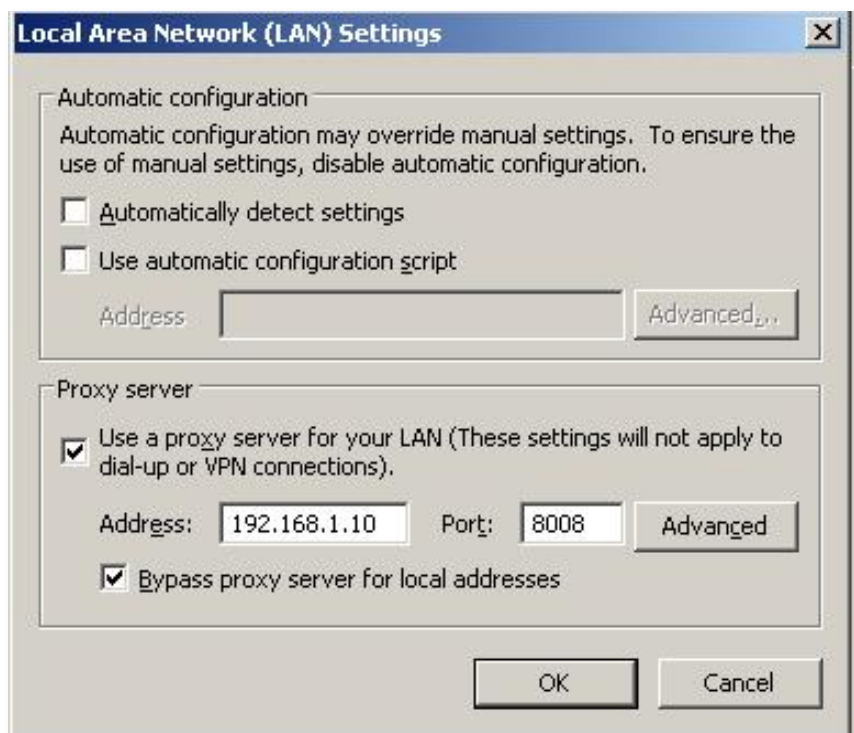


Figure 27 – GPO Local Area Network Settings

9. This setting will now be enforced and the next policy update.

5.7.2.2.2 Manually Setup Proxy Browser Settings

If you are not using the Active Directory/NTLM features, but still want to use the iboss as a proxy filter, you will need to manually setup the Proxy Settings for the browser. To do this with Internet Explorer, click on Tools → Internet Options → Connections Tab → LAN Settings and then check Use a proxy server for your LAN. Enter the IP address of the iboss and the proxy port number (default 8008) and click OK. To do this in Firefox web browser, click Tools → Options → Advanced → Network Tab → Settings Button → Select Manual proxy configuration. Enter the IP address under the HTTP Proxy setting for the iboss IP address and the proxy port (default 8008) and click OK. This will now prompt a user to login before using the Internet.

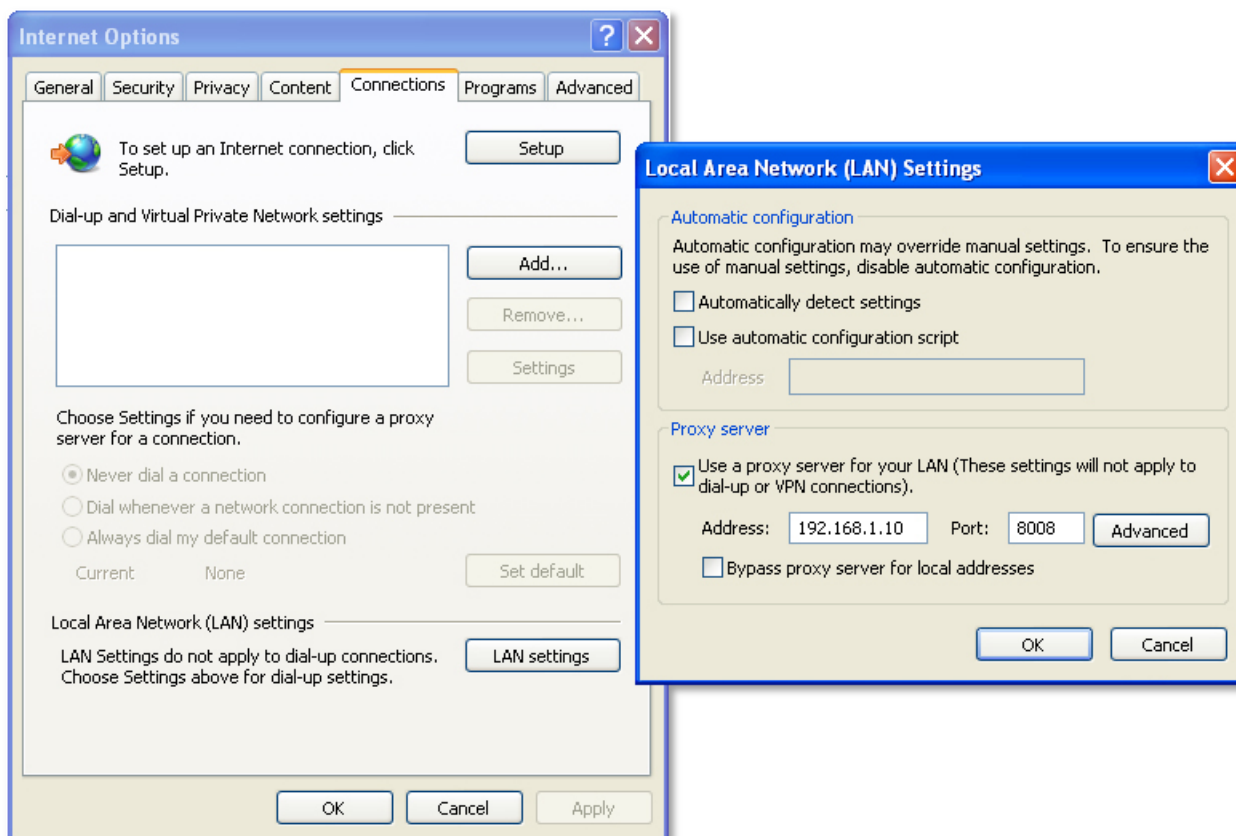


Figure 28 – Manual Proxy with Internet Explorer

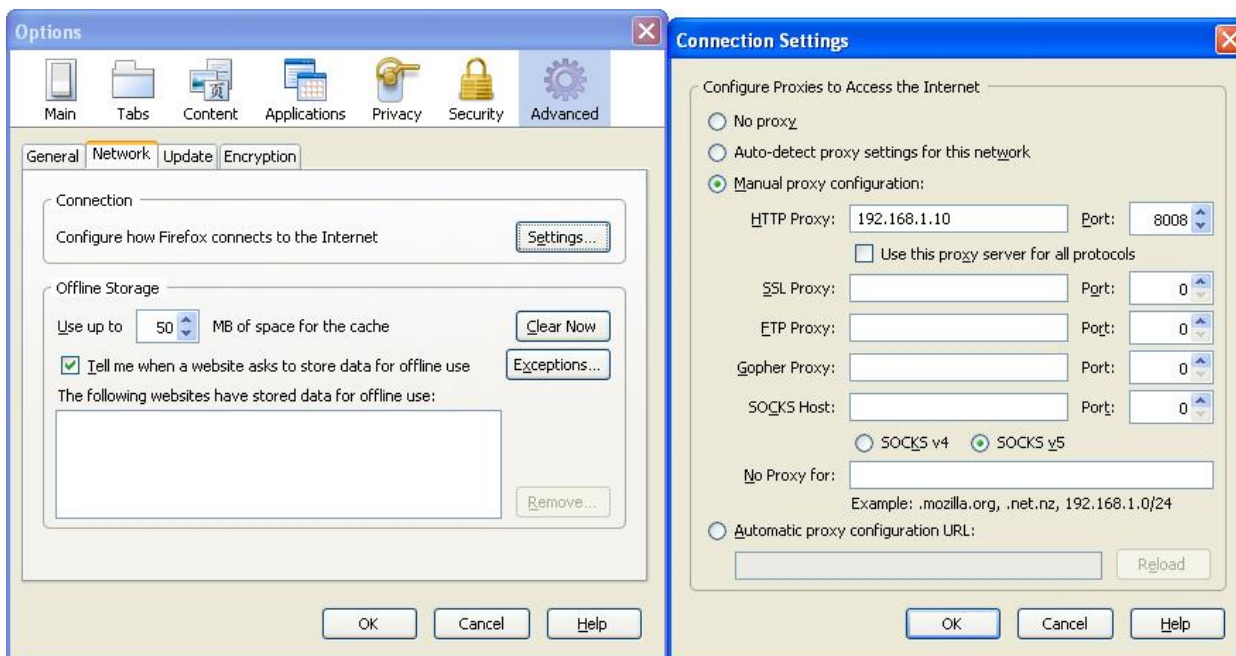


Figure 29 – Manual Proxy with Mozilla Firefox

5.8 Active Directory Plugin/Network Access Controller Integration

Save

Download AD Plugin

+

Global Settings

?

Last Communication Info

Registered AD Servers / NAC Agents

?

Stats

Request Count

0

Successful Request Count

0

Unsuccessful Request Count

0

Delete Selected...

+ Add

Filter...

<input type="checkbox"/>	Name	Description	IP Address	Request Co...	Successful R...	Unsuccessf...	Default Filteri...	Actions
<input type="checkbox"/>	DC01		10.128.16.16				1	
<input type="checkbox"/>	chromesso		127.0.0.1				1	
<input type="checkbox"/>	test	test	1.1.1.1				1	

Figure 30 – AD Plugin / NAC Integration

This feature allows you to configure the iboss to work with the iboss Active Directory plugin. The iboss Active Directory plugin is a service you install on your Active Directory server which communicates user login information with the iboss. The Active Directory plugin is one of two methods to integrate the iboss with your Active Directory domain. You can alternatively use the settings in the "Active Directory & Proxy Settings" page to use logon and logoff scripts to perform Active Directory user authentication. When using the alternative technique, install of the Active Directory plugin is not required.

You may download the latest iboss Active Directory Plugin at:

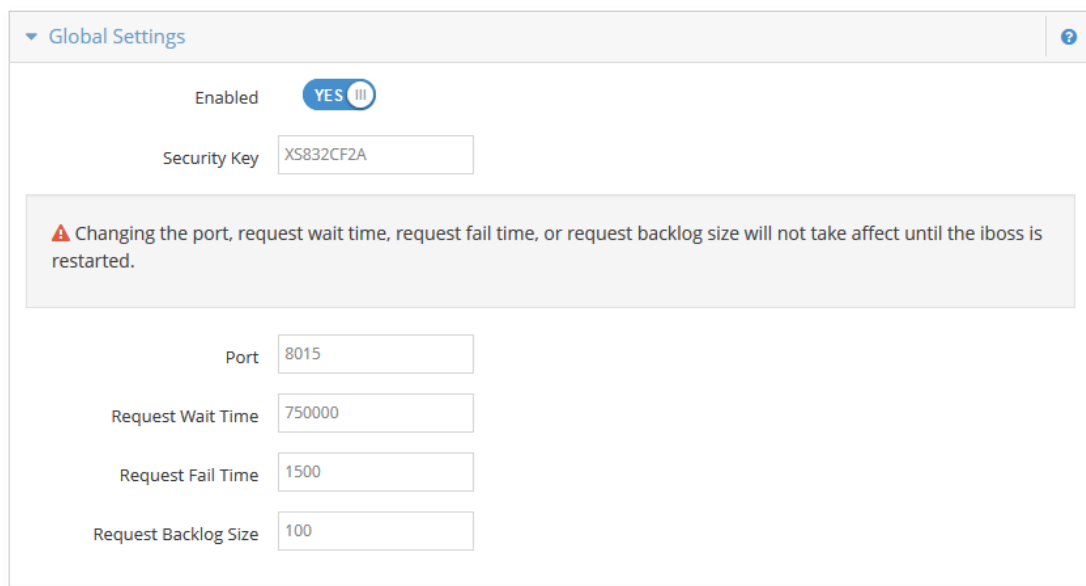
www.iboss.com/adplugin/adplugin.zip

Using the Active Directory plugin has advantages to using logon and logoff scripts as it allows multiple distinct Active Directory domains to report user logon activity to the iboss. When using logon and logoff scripts, the iboss can only be joined to one domain. In addition, the plugin offloads authentication information from the iboss and is more efficient in larger environments.

Register any Active Directory domain which will be communicating to the iboss via the plugin. To remove a cluster member from the list, select the Domain to remove and click the "**Remove**" button located at the bottom of the page. Click the "**Done**" button when you are finished.

Note: In order for your Active Directory domain to communicate with the iboss, they must first be registered below with the correct IP Address. In addition, the security key used in the main settings must match the security key configured in the Active Directory plugin installed on each domain controller.

5.8.1 Global Settings



Global Settings

Enabled **YES**

Security Key XS832CF2A

⚠ Changing the port, request wait time, request fail time, or request backlog size will not take affect until the iboss is restarted.

Port 8015

Request Wait Time 750000

Request Fail Time 1500

Request Backlog Size 100

Figure 31 – AD Plugin – Global Settings

Enable AD Plugin – Enable this option if you are going to be using the Active Directory Plugin

Security Key – This is the security key used to communicate with the domain controller and iboss. They must match exactly.

Note: Changing the port, request wait time, request fail time, or request backlog size will not take effect until the iboss is restarted.

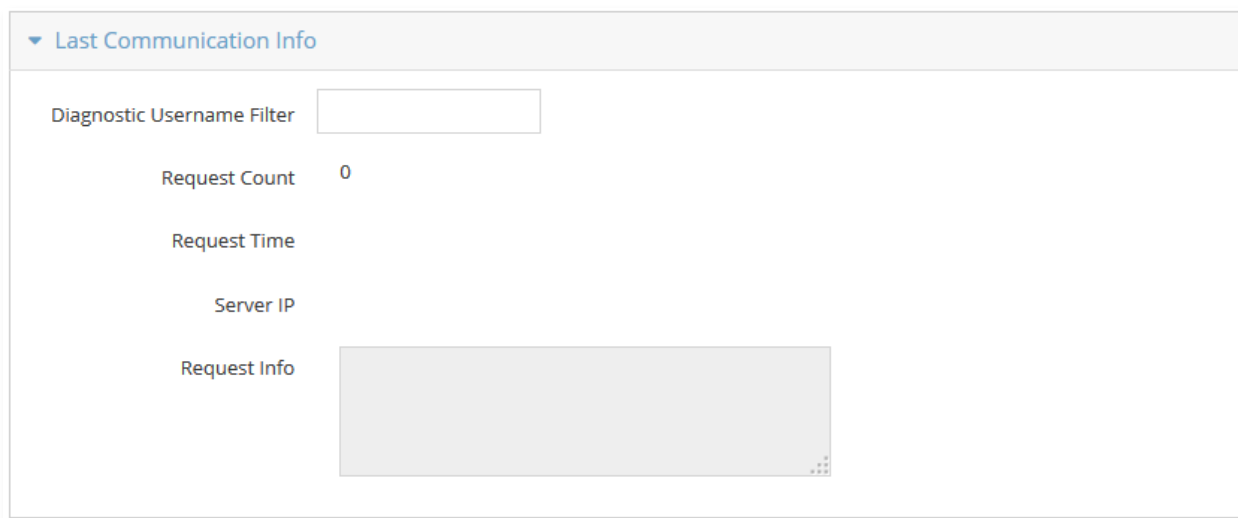
Port – This is the port number used for the active directory plugin. Default is 8015.

Request Wait Time – This is the Request Wait time for how long the Plugin will wait to respond to the iboss.

Request Fail Time – This is the Request Fail time for how long until the request fails to the iboss.

Request Backlog Size – This is the backlog size for requests that are waiting to process.

5.8.2 Last Communication Info



▼ Last Communication Info

Diagnostic Username Filter

Request Count 0

Request Time

Server IP

Request Info

Figure 32 – AD Plugin – Last Communication Info

This section allows you to diagnose what gets sent from the AD Plugin for the username that you specify. Enter the username you wish to diagnose, and click the Apply button. On the next authentication event (login, gpupdate, etc.) it will show you the groups and server information for that particular user.

5.8.3 Registered AD Servers / NAC Agents

5.8.3.1 Stats

Request Count – Current Request Count

Successful Request Count – Current Successful Request Count

Unsuccessful Request Count – Current Unsuccessful Request Count

The list allows you to select particulars server and click Delete Selected button.

To edit an existing server, click the pencil icon to edit the entry.

To add a new server, click the Add button.

5.8.4 Add Active Directory Server

The screenshot shows a dialog box titled "Add AD Server". It contains the following fields and controls:

- Name ***: A text input field.
- Description**: A text input field.
- IP Address ***: A text input field.
- Use Subnet for Default Filtering Group**: A toggle switch currently set to "NO".
- Default Filtering Group**: A dropdown menu currently showing "Group 1".
- Buttons**: "Cancel" and "Save" buttons at the bottom right.

Figure 33 – AD Plugin – Add Active Directory Server

Name – This is for reference of which Active Directory server you are adding.

Description – A description can be added for reference.

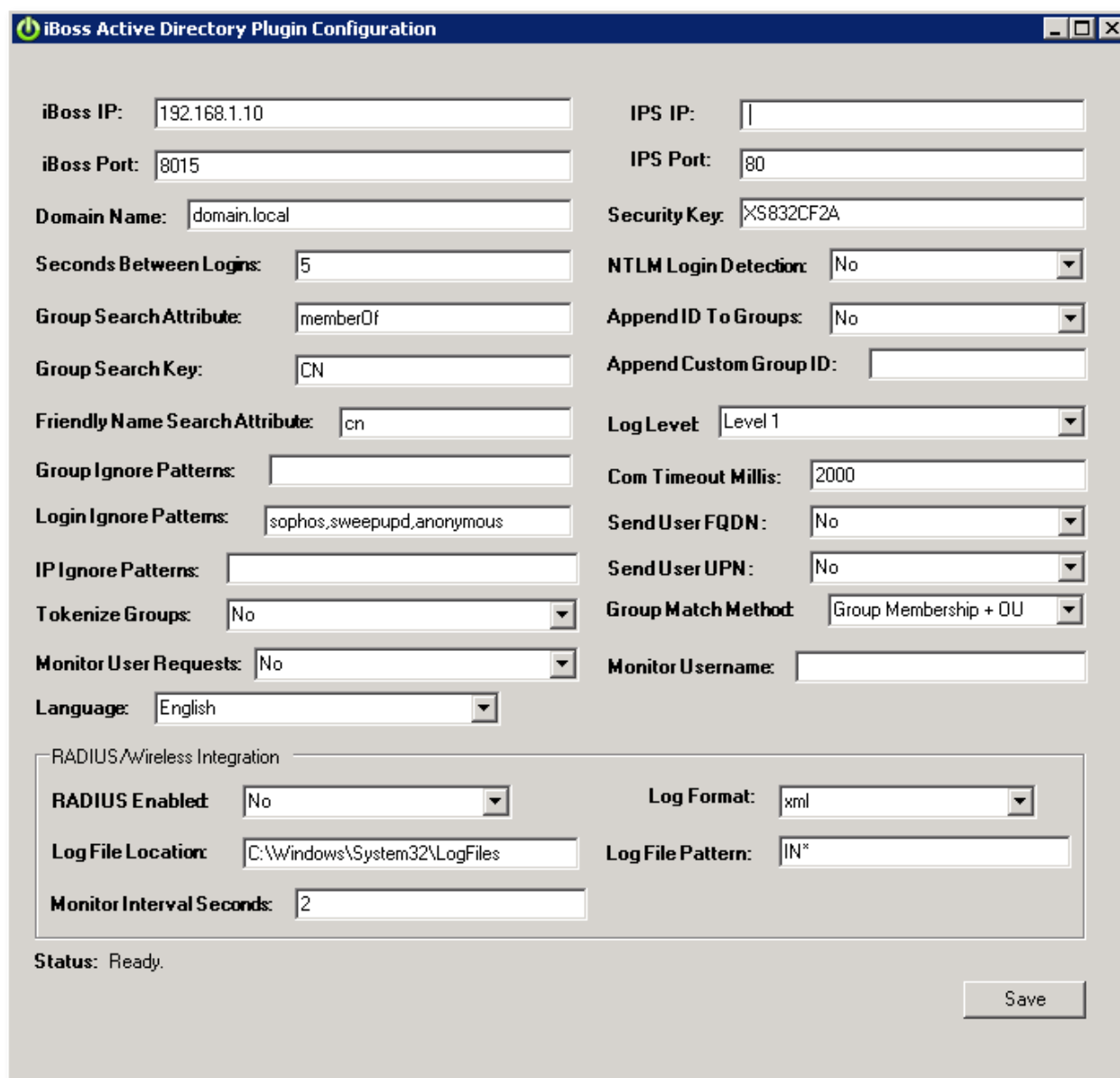
IP Address – This is the IP address of the Active Directory server.

Default Filtering Group – This is the default filtering group for this active directory domain.

Use Subnet For Default Filtering Group – This will either default to the group chosen above or the subnet default filtering group if chosen to yes.

Once finished, click "**Add**" to add the Active Directory server.

5.8.5 iboss Active Directory Plugin Configuration



iBoss IP: 192.168.1.10

iBoss Port: 8015

Domain Name: domain.local

Seconds Between Logins: 5

Group Search Attribute: memberOf

Group Search Key: CN

Friendly Name Search Attribute: cn

Group Ignore Patterns:

Login Ignore Patterns: sophos,sweepupd,anonymous

IP Ignore Patterns:

Tokenize Groups: No

Monitor User Requests: No

Language: English

IPS IP:

IPS Port: 80

Security Key: XS832CF2A

NTLM Login Detection: No

Append ID To Groups: No

Append Custom Group ID:

Log Level: Level 1

Com Timeout Millis: 2000

Send User FQDN: No

Send User UPN: No

Group Match Method: Group Membership + OU

Monitor Username:

RADIUS/Wireless Integration

RADIUS Enabled: No

Log File Location: C:\Windows\System32\LogFiles

Monitor Interval Seconds: 2

Log Format: xml

Log File Pattern: IN*

Status: Ready.

Save

Figure 34 – iboss Active Directory Plugin Configuration

This is the configuration of the iboss Active Directory Plugin. Enter in the information for your iboss. These settings work in conjunction with the Active Directory Plugin configuration within the iboss interface.

iboss IP Address – The local IP address of the iboss.

iboss Port – This is the port used for communication with the iboss. Default is 8015.

IPS IP – This is the IP address of the iboss IPS/IDS device if you have one.

IPS Port – This is the port number to which the AD plugin communicates with the IPS/IDS device.

Security Key – This is the key that matches the Security Key in the iboss (Network → AD Plugin page).

Domain Name – This is the Active Directory Domain that the plugin is on.

Seconds Between Logins – This is the time in seconds the plugin will wait between duplicate login requests.

Group Search Attribute – This attribute is for looking up group names. Default is **memberOf**.

Group Search Key – This is the field within Active Directory where group names are saved.

Append ID To Groups – This is the field that allows you to append the Domain Name to group; [student@domain1.local](#) or append a custom Group ID.

Append Custom Group ID – If append Custom Group ID is chosen above, enter here a custom Group ID to append to the group name.

Friendly Name Search Attribute – This is the field that shows the friendly name of the users.

NTLM Login Detection – This will detect NTLM authentication when users log in.

Log Level – This is the amount of login information will be logged on the Domain Controller.

Group Ignore Patterns – These are words or patterns within the AD group names that you would like the AD plugin to ignore (not sent to iboss).

Login Ignore Patterns – These are words or patterns within the AD username that you would like to be ignored by the AD plugin (not sent to iboss).

IP Ignore Patterns – These are IP addresses that you would like to be ignored by the AD plugin (not sent to iboss).

Com Timeout Millis – This is the communication timeout between the AD plugin and iboss (in milliseconds).

Send User FQDN – Option to send the iboss the user's Fully Qualified Domain name. ex [user@domain.local](#)

Group Match Method – This is the method of how the groups are matched by Security Group or Organizational Unit (OU).

Tokenize Groups – This setting allows you to set wildcards to group names like "Students" that would match groups called Students 2013 & Students 2014.

Monitor User Requests – This option allows you to monitor a specific username in the event viewer.

Monitor Username – This is where you specify which username you would like to monitor (from above)

If a radius server is running on the Domain Controller, the AD Plugin can be configured to send that login information to the filter. For the most part, you only need to Enable the Radius settings and make sure the Log File is DTS Complaint.

NOTE

You may need to Right-click the program under Start and Run as Administrator.

Once finished, click **Save** and close the window. Follow the next steps to audit logon events.

5.8.5.1 Edit AD Plugin Orca

Orca is a Microsoft program that allows you to edit the .msi installer of the AD Plugin before installing. This is beneficial to configure the settings prior to installing the AD Plugin on multiple servers.

First, install the Orca.msi program. Once installed, you can right-click the AD Plugin .msi file and click "Edit with Orca".

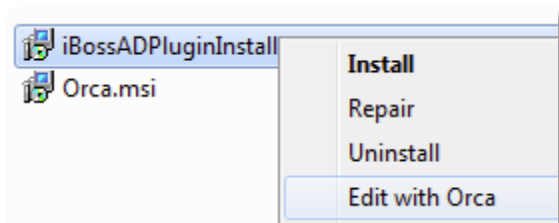


Figure 35 – Edit with Orca option

When it opens in Orca, click on **Property** on the left side and then click on **Property** at the top to sort the options by name.

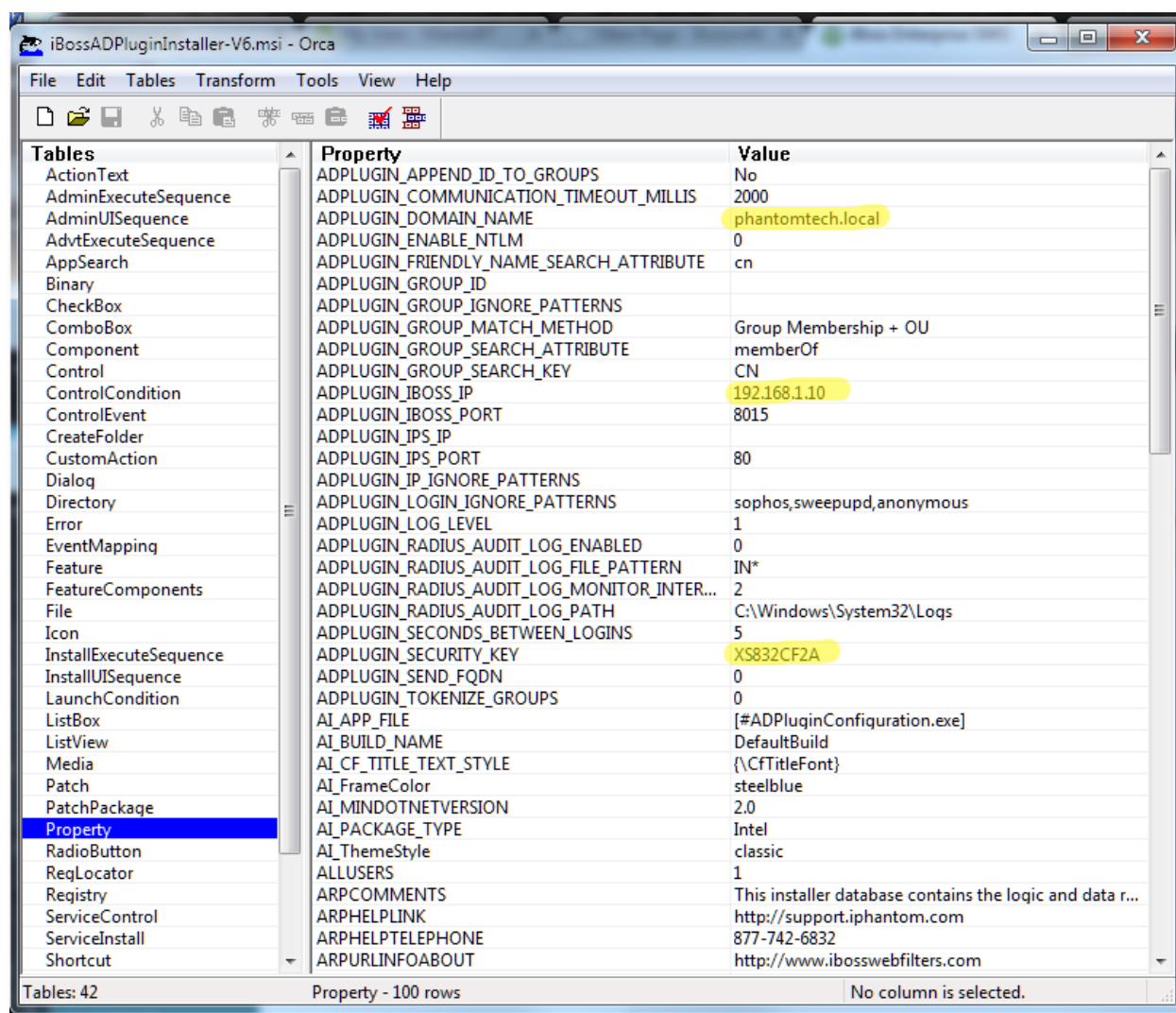


Figure 36 – AD Plugin Properties with Orca

Edit the highlighted fields for the Security Key, IP address of the iboss and the domain.

Once finished, click the **Save** icon or close the program and it will prompt you to Save and click **Yes**.

Do not click **File** and then **Save As**, as this will only save the select property that you have selected.

5.8.5.2 AD Plugin Radius Audit Log

The iboss AD Plugin has the ability to audit logs for Radius Authentication. In the parameters of the AD Plugin installation, there are additional features to modify for the Radius Audit Log. The default Radius Audit Path is at C:\Windows\System32\LogFiles.

ADPLUGIN_RADIUS_AUDIT_LOG_ENABLED	1
ADPLUGIN_RADIUS_AUDIT_LOG_FILE_PATTERN	IN*
ADPLUGIN_RADIUS_AUDIT_LOG_MONITOR_INTERVAL_SECONDS	2
ADPLUGIN_RADIUS_AUDIT_LOG_PATH	C:\Windows\System32\LogFiles

Figure 37 – AD Plugin Radius Audit Log Configuration

5.8.5.3 Active Directory Audit Logon Events

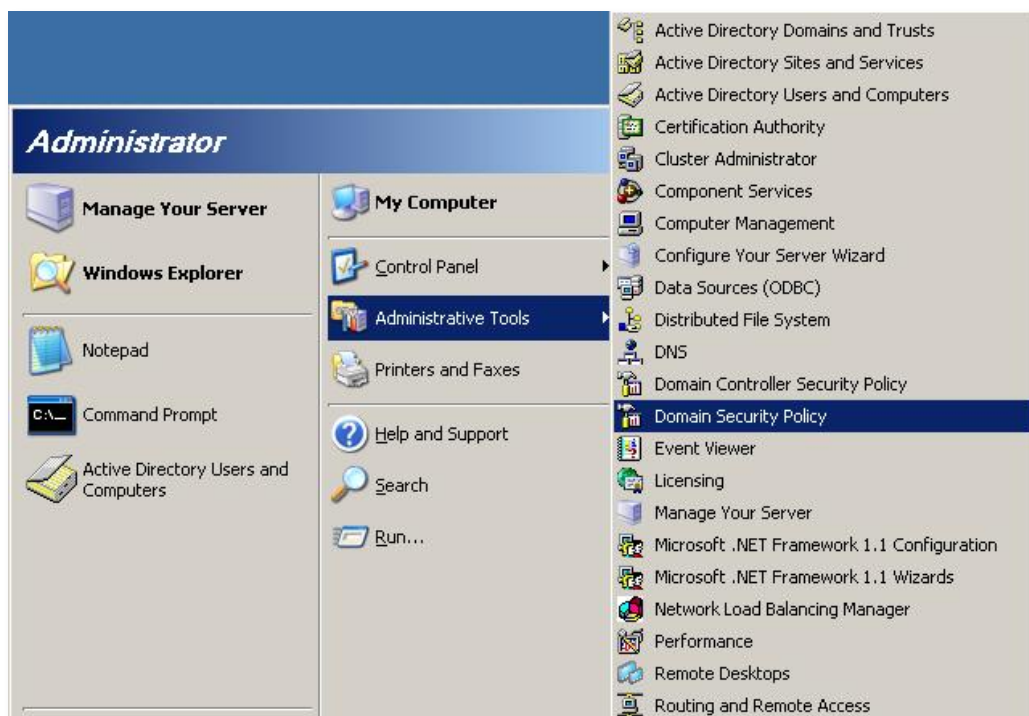


Figure 38 – Domain Security Policy

To ensure the Active Directory Plugin is working correctly, you will need to audit logon events. To do this, click on **Domain Security Policy** within your **Administrative Tools** as shown in the figure above.

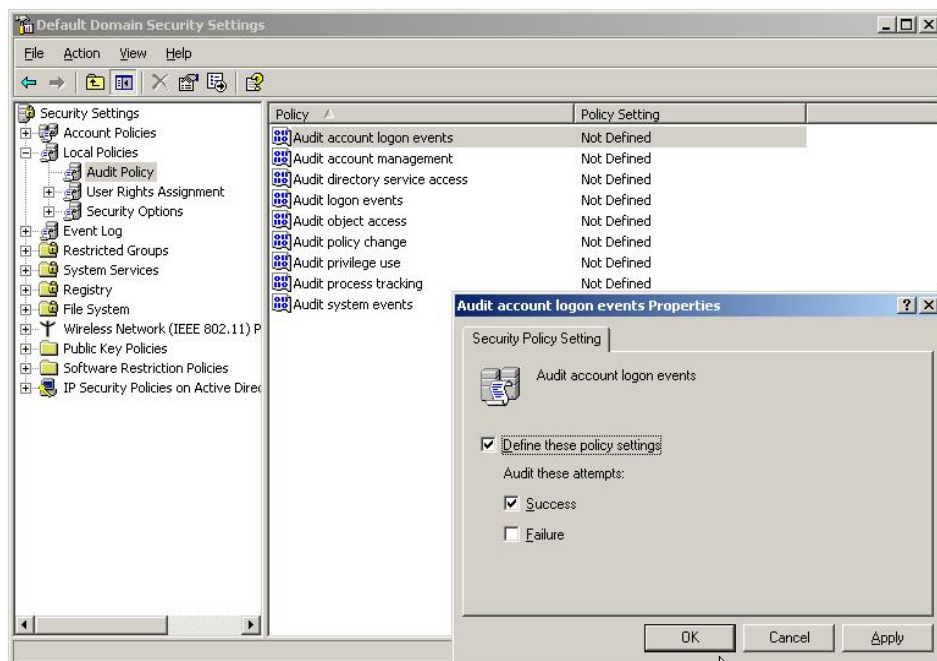


Figure 39 – Audit Account Logon Events

Expand under Security Settings → Local Policies → Audit Policy. Double click the first option **Audit account logon events** and make sure the checkbox for **Define these policy settings** and **Success** is checked and click **OK**.

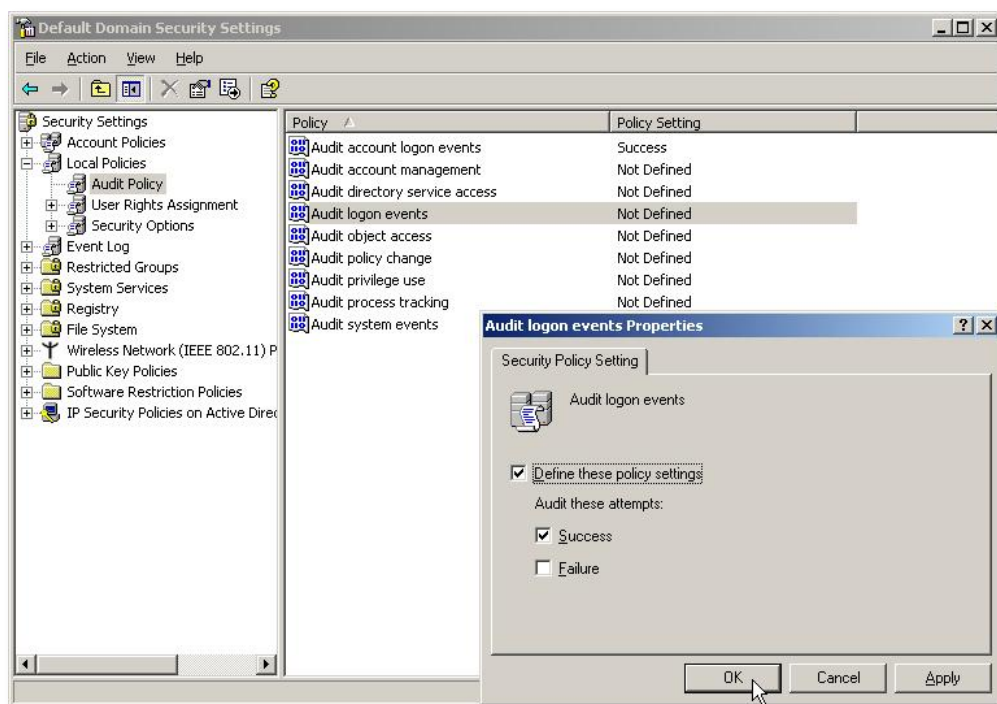


Figure 40 – Audit Logon Events

Next, double-click on **Audit logon events** (4th option down) and make sure the checkbox for **Define these policy settings** and **Success** is checked and click **OK**.

5.8.5.4 NAC Integration

Please see NAC Vender (ex: Enterasys Mobile IAM) iboss Integration Guide for details on integrating with the Vendor NAC. You can obtain this from iboss Support.

5.9 Mobile Client & Local SSL Inspection Agent

Please see iboss Security Agents guide for more details in the iboss Security Agent mobile client install and local SSL Inspection Agent. The agent and guide can be downloaded from the Download Agent button on this page.

Save

Download Agent

Global Settings

Enable Mobile Client Filtering

YES

Enable Local SSL Inspection

NO

Session Timeout

900

⚠

Changing the listening IP, client registration ports (including SSL port), request wait time, request fail time, or request backlog size will not take affect until the iboss is restarted.

Listening IP

Client Registration Port

8025

Client Registration Port (SSL)

8026

Request Wait Time

750000

Request Fail Time

1500

Request Backlog Size

100

Figure 41 – Mobile Client & Local SSL Inspection Agent

Group Specific Settings

Group:

<
Group 1
>

Security Key

29XA3PD231

Extract Group From LDAP

None

Mobile Client Mappings

Stats

Request Count0

Total Processors50

Licensed Nodes0

Ready Processors50

Active Mobile Clients0

Delete Selected...

+ Add

Filter...

	Name	Description	Hardware ID	Filtering Group	Request Count	Actions
<input type="checkbox"/>	test1	test	1234	2	0	
<input type="checkbox"/>	asdf	asdf	asdf	1	0	

Figure 42 – Mobile Client & Local SSL Inspection Agent 2

5.10 ibossNetID Single Sign-On Agent

Please see ibossNetID Install Guide for more details on installing this. The latest document can be obtained for the download link within the iboss interface.

ibossNetID Single Sign-On Agent

Apple Logon Hook
Apple Logoff Hook
ibossNetID SSO Agent

Group: < Group 1 >

Groups Specific Settings

Enable Apple Logon Hooks YES III

Enable ibossNetID Agent YES III

⚠ If "Enable Apple Logon Hooks" is enabled above, download the logon and logoff hook scripts from the toolbar above, then install these scripts as logon hooks on the Apple computers.

If "Enable ibossNetID Agent" is enabled above, download the ibossNetID agent from the toolbar above and deploy to computers on the network.

Group Security Key 8H29DA6N31

Default Group The group a

Extract Group From LDAP None

Query LDAP Only For Logins To Domain

ibossNetID Session Timeout 3600

ibossNetID Replay Window 10800

ibossNetID Source IP Verification YES III

Stats

Total Processors	25	Ready Processors	25
Apple Logon Hook Request Count	0	ibossNetID Request Count	0
Apple Logon Hook Successful	0	ibossNetID Successful	0
Apple Logon Hook Unsuccessful	0	ibossNetID Unsuccessful	0

Save

Figure 43 – ibossNetID Single Sign-On Agent

5.11 eDirectory Settings

eDirectory

eDirectory Settings

Enable User Polling

YES

Full Tree Sync

NO

Ignore Last Login Time

NO

Enable Stats

YES

Enable Login Scripts

NO

Login Scripts Port

8035

Initial User Full Sync

NO

User Login Polling Interval

300

Enable Authentication Delay

NO

Authentication Delay

10

Save

eDirectories

Stats

Polling Count

19

User Polling In Progress

No

Sync Message

Last Users Found Count

0

Queue Count

0

Pending Login

0

Pending Logout

0

Clear Queue

Clear Stats

Download Stats

Actions

+ New eDirectory

Filter...

Figure 44 – eDirectory Settings

5.11.1 iboss eDirectory Transparent Integration

The iboss Enterprise integrates natively with Novell eDirectory servers to provide seamless transparent authentication of users on the network. Integration with eDirectory allows administrators to manage policies based on a user's eDirectory group membership. In addition, integration unifies web filtering administration with an existing Novell eDirectory infrastructure.

Key Features

- Live Real-Time eDirectory event monitoring
- eDirectory user polling support
- Multiple simultaneous eDirectory monitoring support
- Compatible with SUSE and Netware based eDirectory platforms
- Web policy enforcement based on eDirectory group membership

Getting Started

This section describes how to configure the iboss to work within an eDirectory network infrastructure.

5.11.1.1 Overview

The iboss can integrate with eDirectory with two different modes. Only one of the two modes is required and the end result is the same. The eDirectory version must be noted as not all modes are supported on older eDirectory firmware releases. Listed below are the two modes and their description:

Mode 1: eDirectory login/logout event monitoring

In this mode, the iboss monitors login and logout events sent by the eDirectory server in real-time. As users log in and out of their workstations, eDirectory sends these events and iboss uses them to associate the user with the workstation and apply dynamic filtering policy depending on which user is logged into the station. To use this mode, eDirectory 8.7 and above is required.

Mode 2: eDirectory user polling

In this mode, the iboss polls the eDirectory server at the configured interval (usually every 2 minutes) for any users that have logged in within the last interval time. For example, if the polling interval is set to 2 minutes, the iboss will query eDirectory for any users that have logged in within the last 2 minutes (repeating this every 2 minutes). Because this mode is not receiving events in real-time, user association to iboss filtering group can take as long as the configured interval. This mode is supported across all eDirectory versions.

5.11.2 Global Settings

The global settings section contains configuration settings that apply across all registered eDirectory servers. The iboss supports the registration of multiple eDirectory servers with independent settings and allows simultaneous monitoring of all registered servers. The global settings are general settings that apply to all servers.

Enable User Polling

This option specifies whether user polling should be used to process user logins from eDirectory. With polling, the iboss will check for logins within a specified polling interval. If using eDirectory events, this option is not required and can be set to No.

Initial User Full Sync

This option specifies whether the iboss should fully synchronize users from eDirectory with the iboss after an iboss reboot. This option is only available if user polling is enabled. When the iboss is restarted, all users are disassociated and fall within the default filtering policy. With this option, iboss will pull all users from the eDirectory tree after a reboot.

User Login Polling Interval

This is the interval at which iboss will check for any new logon events from eDirectory. At this interval, iboss will query the eDirectory tree for any new logon events that have occurred and associate the user with the eDirectory filtering policy. This option only applies when using eDirectory polling. When using eDirectory events, this option is not used.

5.11.3 eDirectories

This section allows you to view Stats of the eDirectory servers.

Polling Count – This is the current Polling count number.

User Polling In Progress – This indicates whether or not the iboss is polling the eDirectory server for logged in users.

Last Users Found Count – Used to indicate how many new users the iboss found during the last sync with eDirectory. Below the global settings, there is a "Force Sync" button which will cause the iboss to immediately start pulling users from eDirectory and associating them with iboss filtering policy. You can use this status count to determine how many users the iboss found in eDirectory. You should click the "Refresh" button while performing a full synch to get an update on this status.

Queue Count – Number count of the current authentication queue.

Pending Login – Number of the pending logins.

Pending Logout – Number of the pending logouts.

To add a new eDirectory Server click the **+New eDirectory** button.

5.11.4 Insert eDirectory – Server Registration Settings

Insert eDirectory

Name *

IP Address/Host *

Port *389

Admin Username (DN) *

Admin Password *

Common Name Search Attribute *

Username Search Attribute *

Match Group Source *LDAP Attribute

User DN Key

Group Search Attribute *

Group Attribute Value Key

Ignore DN Patterns

Use Full User DNNO

Default Policy *1. 'Group 1'

Connect Timeout20

Network Start IP0.0.0.0

Network End IP0.0.0.0

Monitor EventsYES

Poll User LoginsNO

Allow Full SyncYES

User Polling Search Base

Use SSLNO

Cancel

Save

Figure 45 – Insert eDirectory

This section allows you to add and edit settings for individual eDirectory servers. Typically, you can add the top level master eDirectory replicas. However, if possible, it is recommended that all eDirectory servers to which users authenticate are registered in this section.

The following describes the settings within the eDirectory Info section used to register the eDirectory server.

Name – Use this setting to specify the server name. You can also use a friendly name for the server. This setting does not affect connection to the eDirectory server and is only used for your reference.

IP Address/Host – The IP Address or host name of the eDirectory server.

Port – The port to which the iboss will connect to the eDirectory server. Typically this is port 389 when SSL is not being used and 636 when SSL is being used.

Admin Username (DN) – The username that the iboss will use to search the eDirectory server tree. This user must have search privileges. In addition, if event monitoring is being used, the user must have monitor event privileges set in eDirectory. Typically, a user with administrative privileges is used.

Admin Password – The password for the admin user specified above.

Common Name Search Attribute – The eDirectory LDAP attribute used to extract the full name of the user (First and Last Name). Default: sn

Username Search Attribute – The eDirectory LDAP attribute used to extract the username for the logged in user. Default: cn

Group Search Attribute – The LDAP attribute that the iboss will use to match group membership. When the user is found in eDirectory, the iboss will compare all groups specified in this attribute to the iboss group names. When the iboss finds a match, the iboss will associate the user with that iboss filtering group policy. If a user is part of more than 1 group that matches an iboss group name, the iboss will use the group with a lower group number (Group 1 match will override Group 3 match). Filtering group names can be found in Home → Identify Computers & Users → Groups Tab. Make sure to name the iboss group exactly like the eDirectory group name that you would like to match. Default: groupMembership

Group Attribute Value Key – When the group search attribute above is found (for example groupMembership), this value specifies the tokens that separate the group names. For example, using the default value of cn, the groupMembership LDAP attribute looks like cn=Staff,cn=Wireless User. With cn in this option, the groups that the iboss would extract are Staff and Wireless User. It would then compare those to the iboss groups. Default: cn

Location Attribute – An optional LDAP attribute that can be used to specify the user's location for generating reports. Typically this is left blank.

Ignore DN Pattern – The iboss will ignore any user logins/logoffs that contain the patterns specified in this option. Any automated service accounts should be specified here. If they are not, whenever the service account (such as an antivirus account) logs into a computer that contains a logged in user, that username will

override the logged in user. Eventually, it will appear as if the service account is the only user logged into the network. Enter these automated user accounts here so that whenever the iboss receives a logon or logoff event from these users, it ignores them and preserves the currently logged in user. Values should be specified separated with a comma.

Default Filtering Policy – If the iboss cannot find a matching iboss group name to eDirectory group name, this specifies the default policy the iboss should apply to the user.

Connect Timeout – This is the timeout (specified in seconds) that the iboss should use when connecting to an eDirectory server. If an eDirectory server is down, this will prevent the iboss from waiting too long before trying to connect again. Default: 20

Monitor Events – Specifies whether eDirectory event polling should be used for this server. This is recommended as login and logout events will be sent in real-time to the iboss.

Poll User Logins – Specifies whether the iboss should use the polling method to poll the eDirectory server for login events. The settings specified in the global settings apply to this mode. This is typically set to No when Monitor Events is set to Yes as the iboss will receive login/logout events in real-time.

Allow Full Sync – Specifies whether this server will participate in the full user synchronization triggered when "Force Full Sync" above is clicked. Typically, set this to "Yes" only for the master eDirectory replica as not all servers need to be queried during a full sync.

User Polling Search Base – This is the level in the eDirectory tree the iboss should use to search for logged in users. When using "Force Full Sync" or enabling the option for "Poll User Logins", this value is required. Typically this is set to the top of the tree (for example, o=iboss).

User SSL/SSL Certificate – This option specifies whether the iboss should use SSL to connect to the eDirectory server. Typically SSL for eDirectory communicates via port 636 and this should be configured in Port Settings. When using SSL, paste your SSL certificate by extracting the contents of the certificate in PEM format. SSL is not required and involves more maintenance as you must monitor your certificates expiration dates to confirm that your certificates do not expire. If your certificate expires, the iboss will no longer be able to communicate with the eDirectory server and the certificate will have to be updated. The default setting for use SSL is usually set to "No"

Add the eDirectory Server – Once you have configured all of your settings, click the Add button to add the server to the registered eDirectory list.

You should refresh the page using the "Refresh" button after adding the server. This will update the "Status" field for the server that was just added to the list. You will want to confirm that the status is "Running..." for eDirectory servers registered to receive eDirectory events and no error is specified.

Conclusion

Once all of your eDirectory servers are registered, you can seamlessly manage policies within the iboss and manage group membership in your eDirectory server. The iboss will dynamically apply the appropriate policy whenever the user logs in using their eDirectory login credentials.

5.12 Clustering

Clustering

Local Settings

Enabled: YES

Node Type: Slave

Retry Sync Interval: 5

Response Timeout: 15

Clustering Port: 17500

Login Clustering Port: 17501

Security Key: 8247E530928B75839485

Master IP Address: 192.168.1.150

Save

Cluster Members

Stats

Total Request Count	0	Total Request Fail	0
Total Request Success	0	Total Heartbeat Requests	0
Total Login Requests	0	Total Logout Requests	0
Total Sent Messages	0		

Actions

+ New Cluster

Filter...



Name	Description	Type	Ip Address	Port	Login Port	Timeout	Actions
My Cluster	This is a cluster	Slave	10.10.10.10	17500	17501	15	 

Figure 46 – Clustering

This feature allows you to configure clustering for a group of iboss filters. By clustering iboss filters, you can have settings from an iboss master automatically replicate across all members of the cluster. This allows a central management point for a group of iboss web filters.

NOTE

All members of a cluster must be of the same model with the exception of comparable x50/x500 and x60/x600 models. For example, a 14500 and 14600 can cluster, but not a 14500 and 4500.

Enter information about cluster members in the required fields and click the **"Add"** button. To remove a cluster member from the list, select the iboss to remove and click the **"Remove"** button located at the bottom of the page. Click the **"Done"** button when you are finished.

NOTE	When creating the cluster, designate a single iboss in the cluster as the master. This will be the iboss which you want to use as the central point for configuring settings. Only the master needs to have cluster members added below. You can also select which settings you will want to replicate from the master to the slaves.
-------------	---

5.12.1 Local Settings

Enable Clustering – This option turns on clustering globally.

Node Type – This field specifies the device node type whether it is a slave or master iboss device.

Retry Sync Interval in Seconds – This field is the interval which the settings are synced.

Response Timeout in Seconds – This field determines how long until the filter waits before deciding that a slave has timed out.

Clustering Port – This field specifies the port used for syncing settings.

Login Clustering Port – This field specifies the port used for syncing logins.

Note: The security key must be 32 hex characters. Valid characters are 0–9 and A–F.

Security Key – This field specifies the security key used when communicating with other clustered iboss devices.

Master IP Address – This field specifies the master iboss IP address of the cluster.

5.12.2 Cluster Members

Stats:

Total Request Count – This is the number of the sync request count.

Total Request Success – This is the number of the sync request successful count.

Total Login Requests – This is the number of the login request count.

Total Sent Messages – This is the number of the sent messages count.

Total Request Fail – This is the number of the request failed count.

Total Heartbeat Requests – This is the number of the heartbeat request count.

Total Logout Requests – This is the status of the logout request count.

5.12.3 Add Cluster Member

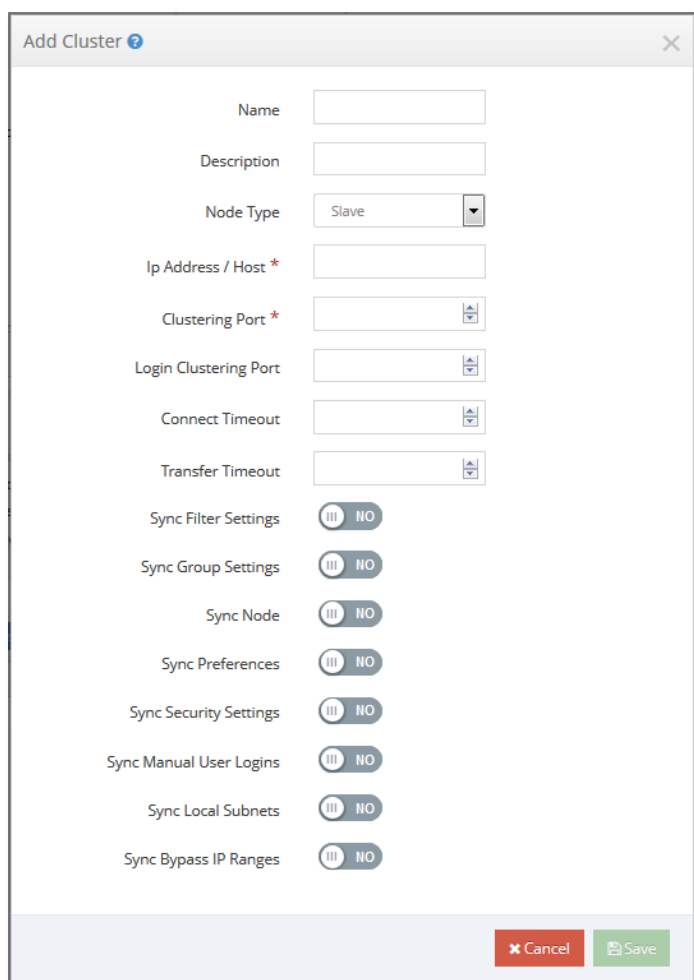


Figure 47 – Clustering – Add Cluster Member

Name – This field is to put the name of the iboss you are adding for reference.

Description – This is the description for the iboss device you are adding.

Node Type – This field indicates whether this device is the master or slave.

IP Address/Host – This field is for the IP of the iboss you are adding.

Port – This is the port number that is used to communicate.

Login Clustering Port – This is the port number that is used to send Login information on.

Connect Timeout – This is the timeout if the response is taking too long.

Transfer Timeout – This is the timeout if the transfer is taking too long.

Sync Filter Settings – This is option to sync the filtering settings.

Sync Group Settings – This is the option to sync groups.

Sync Nodes – This is the option to sync computer nodes.

Sync Preferences – This is the option to sync preference settings.

Sync Security Settings – This is the option to sync security settings.

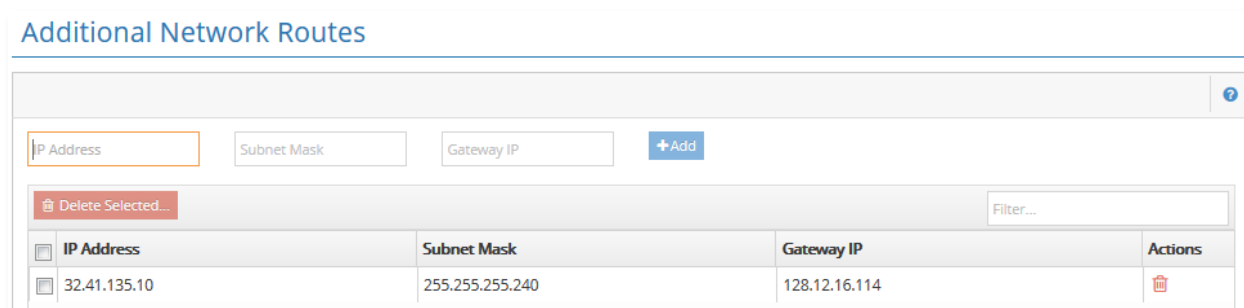
Sync Manual User Logins – This is the option to sync manual logins across filters. **Note:** To use this, all filters will need all other filters set up as Cluster Members.

Sync Local Subnets – This is the option to sync the local subnets

Sync Bypass IP Ranges – This is the option to sync bypass IP Ranges.

Once finished, click the “**Save**” button to add the iboss cluster device.

5.13 Add Additional Routes



IP Address	Subnet Mask	Gateway IP	Actions
32.41.135.10	255.255.255.240	128.12.16.114	

Figure 48 – Add Additional Routes

Ideally no Additional Routes should be needed, except under special circumstances where a 2 port, in-line iboss interface is inaccessible on a layer-3 network. You’d need to configure the iboss Gateway IP Address to be the core router (instead of the firewall). The routes have nothing to do with the flow of traffic with regard to filtering. These routes are specifically designed to alleviate problems in accessing the iboss web configuration interface when the iboss is installed in-line on the network.

On a layer 3 network where there is a core router/switch and an external firewall, typically the gateway IP Address of the iboss is configured to be the internal router (under the Internet Connection section where the iboss IP Address is configured). This alleviates the need to add additional routes as the core router is responsible for routing all traffic into the network and out to the Internet. However, on a layer 3 network with the same topology, if the iboss Gateway IP Address is configured to be the outside firewall, that firewall may not have the routing rules to route internally destined traffic back to the local computers. In this case, an additional route would be required.

Suppose the following scenario:

Firewall: 10.0.0.1

Core Router: 10.0.0.254

iboss IP: 10.0.0.100

iboss Gateway IP: 10.0.0.1

In this case, the route that should be added would look like:

10.0.0.0/255.0.0.0 → 10.0.0.254

5.14 Bypass IP Ranges

Bypass IP Addresses


General Settings

Bypass Citrix Applications

NO

Save

IP Bypasses


Note: Do NOT set Full Bypass to "Yes" if the IP range being entered represents local IPs and it contains internal DNS servers. Local DNS servers entered in the bypass IP Range will not be blocked but their requests will still be analyzed and used internally by the iboss SWG. Only enter local IP ranges that include DNS servers if you are sure you want to completely bypass those servers from iboss visibility.

Adding IP Ranges below does not exclude the IP Addresses from Gateway SSL/HTTPs Decryption. If you have Gateway SSL decryption enabled, make sure the subnets the IP Addresses belong to have SSL Decryption disabled or add the IP Address subnet to the bypass list in the SSL Gateway Decryption section.

Standard E

IP Address Start

IP Address End

Note

+ Add

Delete Selected...

Filter...













<input type="checkbox"/>	Bypass Type	IP Address ...	IP Address ...	IPv6 Address	IPv6 Subne...	Note	Actions
<input type="checkbox"/>	Standard Bypass	10.128.16.205	10.128.16.205				
<input type="checkbox"/>	Full Bypass	10.128.17.142	10.128.17.142				
<input type="checkbox"/>	Standard Bypass	10.128.18.240	10.128.18.240				
<input type="checkbox"/>	Full Bypass	10.128.17.148	10.128.17.148				
<input type="checkbox"/>	Standard Bypass	208.70.74.17	208.70.74.17			help.iboss.c...	
<input type="checkbox"/>	Standard Bypass	10.128.31.198	10.128.31.198				
<input type="checkbox"/>	Standard Bypass	10.128.31.235	10.128.31.235				
<input type="checkbox"/>	Standard Bypass	10.128.16.156	10.128.16.156				
<input type="checkbox"/>	Full Bypass	10.128.24.55	10.128.24.55				
<input type="checkbox"/>	Standard Bypass	10.128.16.78	10.128.16.78			JS	
<input type="checkbox"/>	Standard Bypass	10.128.16.79	10.128.16.79			Kimberly	
<input type="checkbox"/>	Standard Bypass	10.128.16.76	10.128.16.76				

Figure 49 – Bypass IP Range

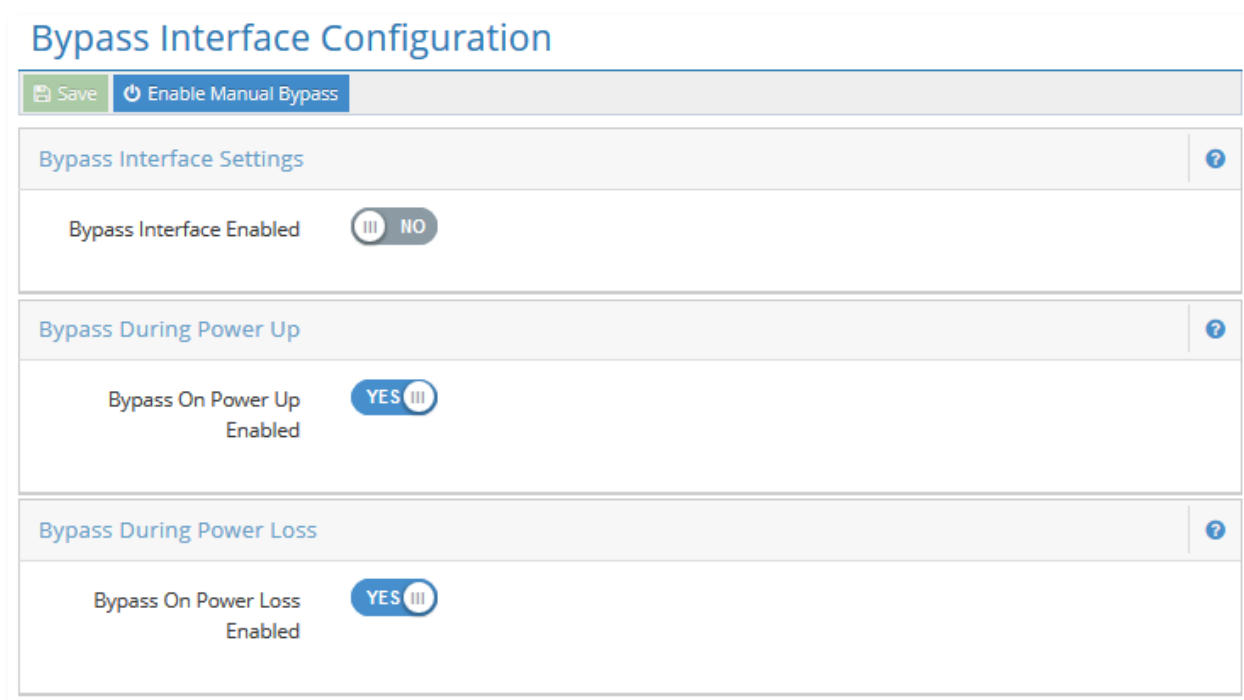
This page allows you to add IP Addresses that you would like to be completely bypassed by the iboss filtering engine. IP Addresses listed here will not appear in your Unidentified Computers list and will completely bypass

filtering. This is useful for bypassing IP Address ranges that include servers, VOIP based phones, and other devices which do not require filtering.

Enter the IP Address ranges below, select the type of bypass, and click the **"Add"** button. A Standard Bypass will work most of the time. A Full Bypass will also bypass the DNS changes associated with Google and YouTube. Bypass but Apply Bandwidth Shaping/QOS removes the IP from filtering, but keeps it for bandwidth control.

To remove an IP Address range from the list, select the range to remove and click the **"Remove"** button located at the bottom of the page. You can add up to 50 IP Address ranges to bypass. Click the **"Done"** button when you are finished.

5.15 Bypass Interface



Bypass Interface Configuration

Save Enable Manual Bypass

Bypass Interface Settings ?

Bypass Interface Enabled NO

Bypass During Power Up ?

Bypass On Power Up Enabled YES

Bypass During Power Loss ?

Bypass On Power Loss Enabled YES

Figure 50 – Bypass Interface Configuration

This page allows you to configure settings if you have a fail-safe Bypass Card installed on the SWG device.

Enable Manual Bypass button – This button allows you to enable the Bypass card bypassing the SWG filtering rules.

Bypass Interface Settings – This option allows you to enable the Bypass Card.

Bypass During Power Up – This option allows the bypass card relay to be flipped to allow traffic to flow through the SWG device during power up.

Bypass During Power Loss – This option allows the bypass card relay to be flipped to allow traffic to flow through the SWG device during power loss.

5.16 Add Additional Local Subnets

Local Subnets/IP Ranges

Local Subnets

Actions: [+New Local Subnet/IP Range](#) Filter...

Type	Filtering Method	Default Policy	Authentication Method	Bandwidth Accounting	Subnet Reporting	Reporting Group #	SSL	Lock Subnet	Subnet/Range	Actions
<input type="checkbox"/> Subnet	IP Address	1	Fixed	N	N	0	N	N	10.0.0.0/255.0.0.0	
<input type="checkbox"/> Range	IP Address	60	Fixed	N	N	0	N	Y	10.20.20.0-10.20.20.255	
<input type="checkbox"/> Range	IP Address	-1	Fixed	N	N	0	N	N	10.30.30.0-10.30.30.255	

Figure 51 – Add Additional Local Subnets

This feature allows you to add and define local subnets. Traffic between local subnets are not filtered by the iboss. In addition, the iboss will only filter Internet traffic from subnets that are defined below. Be sure to include all the subnets on the local network.

5.16.1 Overview

You can add a top level subnet (such as 10.0.0.0/255.0.0.0) if your network includes many smaller subnets and you would like to have the entire subnet on the same default policy.

In addition, you can select to add IP Ranges if you would like to assign a default policy to a specific IP Range. When the default policy for a subnet is determined, the iboss will start from the subnet at the top of the list and work its way down. The iboss will always traverse all subnets from top to bottom. Any subnet (or IP Range) toward the bottom of the list will override subnets toward the top of the list and the default policy for subnets lower in the list will override the default for subnets at the top of the list for matching IPs.

It is recommended that IP Subnets are used instead of IP ranges. If there is a range of IPs that must have a separate default policy from the top level subnet, add the subnet first that contains the IP range, then add the IP range within that subnet lower in the list.

Authentication Method – The recommended option is **"Fixed"**. With this option the iboss presents the user with the iboss login page if **"Require User Login"** is selected as the default policy and the user has not been authenticated (transparently or by other methods). The iboss login page will NOT be presented if the user was authenticated transparently or the default policy is not **"Require User Login"**. Selecting **"Active Directory/NTLM"** will cause the iboss to attempt single sign-on/NTLM if the user was not authenticated transparently.

The **"Bandwidth Accounting"** option specifies whether the iboss should track bandwidth statistics for the subnet or IP range. If there are overlapping subnets or IP ranges in the list, disable the **"Bandwidth Accounting"** option for the duplicate subnet so that bandwidth is not accounted for twice which will inflate bandwidth statistics.

Enter the local subnets and click the **"Add"** button. To remove a subnet from the list, select the subnet to remove and click the **"Remove"** button located at the bottom of the page. Click the **"Done"** button when you are finished.

Filtering Method Option – The iboss has the ability to filter a subnet based on a variety of methods.

IP Address – This option indicates that IP Addresses should be used to apply a filtering policy to traffic originating on this subnet. With this option, you can apply policies to individual IP Addresses, but not directly to a computer based on its MAC address within the subnet. In addition, if using Active Directory NTLM/Single Sign-on, you will still have the ability to determine the user that was generating the network traffic, but you will not be able determine which computer (based on its MAC address) the user was operating when generating the traffic.

MAC Address – Filtering policies on this subnet are based on the Mac Address (MAC) of the computer's network adapters. This allows you to identify computers on your network uniquely and assign computers to different filtering groups. If using Active Directory NTLM/Single Sign-on, this method also allows you to identify which computer a user was accessing when network activity occurs. This feature gives you more visibility on the network, especially in a NTLM/Active Directory environment, as it allows you to not only identify the user but associate the station that was used to generate the network traffic. This option indicates that traffic originating from this subnet does not traverse any internal routers or gateways.

MAC Address Through Gateway – This option has the same effect as the "MAC Address" option above, except it should be chosen if traffic originating from this subnet traverses an internal gateway or router before reaching the iboss. You must register the internal gateway or router with the iboss through the "Register Internal Gateways" menu option (under Main Menu→Setup Network Connection).

To add a new range or local subnet, click the **New Local Subnet/IP Range** button.

5.16.2 Insert Local Subnets/IP Ranges

The screenshot shows a configuration window titled "Insert Local Subnet". It contains the following fields and controls:

- Type ***: A dropdown menu with "Range" selected.
- IP Start ***: An empty text input field.
- IP End ***: An empty text input field.
- Authentication Method ***: A dropdown menu with "Fixed" selected.
- Filtering Method ***: A dropdown menu with "IP Address" selected.
- Default Policy ***: A dropdown menu with "Require user login on this Subnet" selected.
- Login Page Group ***: A dropdown menu with "1. 'Group 1'" selected.
- Bandwidth Accounting**: A toggle switch set to "NO".
- Use Subnet Reporting Group**: A toggle switch set to "NO".
- Subnet Reporting Group #**: A text input field with "0" and up/down arrow buttons.
- Lock Subnet Policy**: A toggle switch set to "NO".

At the bottom right of the window are two buttons: a red "Cancel" button and a green "Save" button.

Figure 52 – Insert Local Subnet

Type – This is the option to choose whether it is a Subnet, Range, or IPv6 Subnet.

IP Start (Range option) – This is the start IP address of the IP range you are adding.

IP End (Range option) – This is the end IP address of the IP range you are adding.

IP Address (Subnet option) – This is an IP address of the IP subnet you are adding; typically you enter the broadcast address.

Subnet Mask (Subnet option) – This is the subnet mask for the IP subnet you are adding.

Authentication Method – This is the option whether to authenticate with fixed filtering or NTLM with Active Directory.

Filtering Method – This is the option to choose whether this IP range or subnet are filtered and identified by IP address, Mac Address, or Mac Address through an internal gateway.

Default Policy – This is the default filtering policy for the IP range or subnet you are adding.

Login Page Group – This is the Login group page for user login used for the IP range or subnet you are adding.

Bandwidth Accounting – This option is to choose whether to account for bandwidth for the IP range or subnet you are adding.

Use Subnet Reporting Group – This setting overrides the Reporting Group setting in the Group section.

Subnet Reporting Group – This setting determines which reporting group data from the subnet will go in to.

Lock Subnet Policy – This setting will prevent the group settings for this subnet from being overridden by a login.

5.17 Register Internal Gateways

Register Internal Gateways

Global Settings

Enabled: **YES**

Gateway Sync Interval: 60

Save

Internal Gateways

Actions **+New Gateway** Filter...

	Gateway Name	Gateway Type	Gateway IP A...	Gateway Prot...	Gateway Description	Actions
<input type="checkbox"/>	test	Cisco	1.1.1.1	TELNET		

Figure 53 – Register Internal Gateways

This page allows you to register gateways that are internal to your network (on the LAN side of the iboss). Typically the iboss is placed between a Layer 2 switch and the network Gateway/Firewall. If your network has any additional internal (non-NAT) gateways that are used to route internal local subnets, you can register those gateways here. The iboss will automatically integrate with the internal gateways so that you may identify and apply filtering rules to computers behind the gateway based on Mac address.

5.17.1 Overview

The global settings apply to all internal gateways added. You must enable internal gateway integration in the global settings for any of the settings on this page to take effect.

Next, enter the internal gateway information and click the "Add" button. To remove a gateway from the list, select the gateway to remove and click the "Remove" button located at the bottom of the page. You can add up to 1000 internal gateways. Click the "Done" button when you are finished.

Note – Do not add any gateways if your network is configured with a single outer gateway. Place the iboss between the outer gateway/router and the internal switch to which all of the computers are connected.

If you register internal gateways on this page, you must add the subnet which is routed by this gateway on the "Additional Local Subnets" page. When adding the additional local subnet, make sure the filtering method "Mac Address through Gateway" is selected.

The global settings apply to all internal gateways added. **You must enable internal gateway integration in the global settings below for any of the settings on this page to take effect.**

Enter the internal gateway below and click the "Add" button. To remove a gateway from the list, select the gateway to remove and click the "Remove" button located at the bottom of the page. You can add up to 1000 internal gateways. Click the "Done" button when you are finished.

NOTE	Do not add any gateways if your network is configured with a single outer gateway. Place the iboss between the outer gateway/router and the internal switch to which all of the computers are connected.
-------------	--

If you register internal gateways on this page, you must add the subnet which is routed by this gateway on the "Additional Local Subnets" page. When adding the additional local subnet, make sure the option "Routed Through Gateway" is set to yes.

5.17.2 Global Settings

These are the global settings for adding an Internal Gateway.

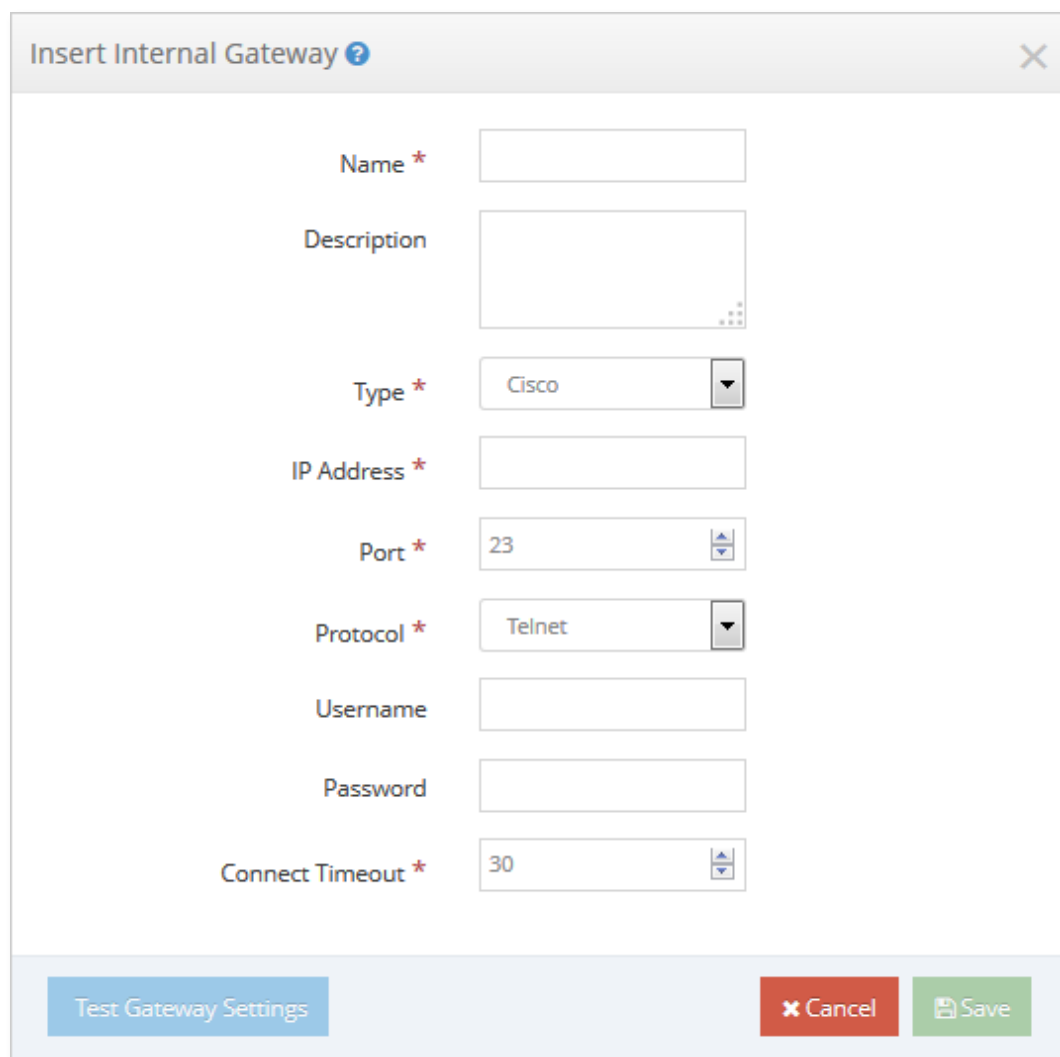
Enable – This is the option to globally turn on this feature.

Gateway Sync Interval – This is the sync interval with the gateways that are adding in seconds.

Once you have changed any of these options, click the "**Save**" button.

To add a new internal gateway, click the **New Gateway** button.

5.17.3 Insert Internal Gateway



Insert Internal Gateway ?

Name *

Description

Type *

IP Address *

Port *

Protocol *

Username

Password

Connect Timeout *

Test Gateway Settings Cancel Save

Figure 54 – Insert Internal Gateway

Name – This is the name for reference for the gateway you are adding.

Description – This is the field to add a description for the gateway you are adding.

Gateway Type – This is the gateway type. Options are **Cisco, HP Switch, Linux, Cisco FWSM, and D-link Switch.**

IP Address – This is the IP address for the internal gateway you are adding.

Port – This is the port used for communication, typically it is port 23 for telnet communication or port 22 for SSH communication.

Protocol – This is the option to choose whether communication is through telnet or SSH.

Username – This is the username to log into the internal gateway.

Password – This is the password to log into the internal gateway.

Connect Timeout – This is the connection timeout if no response is received specified in seconds.

Once you have finished adding these settings click the **“Test Gateway Settings”** button. To save the settings, click the **“Save”** button. It will add it to the Internal Gateways list.

To remove entries click the **“Remove”** button next to the gateway entry.

5.18 Edit Advanced Network Settings

Advanced Settings

Save

General Settings

UDP Destination Port

8000

UDP Source Port

8001

Always On Connection

NO

Aggressive TCP Latching

NO

YouTube SSL Blocking

NO

IPv6 Packet Processing

Disabled Globally

Group Cache Settings

Disable AD Plugin / ibossNetID / Apple Hooks Cache

NO

Disable AD Login Cache

NO

Disable Mobile Login Cache

NO

Figure 55 – Edit Advanced Network Settings

5.18.1 General Settings

The iboss connects to the iboss servers via UDP. You may select which ports it connects through. The default destination port is 8000 and default source port is 8001.

Always On Connection – This option allows you to still have Internet access even if it loses connection with our servers. This function will work after the first time that it has established a connection.

Aggressive TCP Latching – Default is disabled (used for filters in Tap-mode to stop users from accessing blocked encrypted sites by repeatedly refreshing the page)

YouTube SSL Blocking – Enables SSL blocking for YouTube. Default is Version 2.

IPv6 Packet Processing – This option will need to be enabled to filter traffic from IPv6 addresses.

5.18.2 Group Cache Settings

Disable AD Plugin / ibossNetID / Apple Hooks Cache, Disable AD Login Cache, Disable Mobile Login Cache – By enabling these options, you are telling the iboss not to cache the login information for that way of authenticating. This way, if a change is made either in your active directory groups or the filtering groups within the iboss, the changes will reflect right away (or the next time the authentication tool checks in with the iboss).

6 Installing the iboss on the Network

Once the network settings have been configured, the iboss is ready to be installed on the network. The two ports you will be using are the “LAN” port and the “WAN” port located on the back of the iboss.

6.1 Transparent Inline Bridge

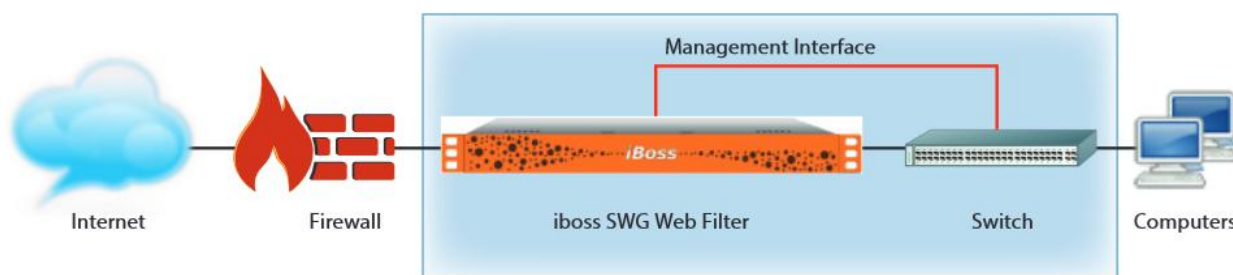


Figure 56 – iboss Hardware Installation

Place the iboss between an existing switch on the network and an existing firewall. For example, if the network has a switch to which computers are connected to, and that switch is connected to the network firewall, the iboss will be placed between the switch and the firewall.

Disconnect the switch from the firewall and connect the switch to the “LAN” port on the iboss. Connect the firewall to the “WAN” port on the iboss.

This completes the physical installation of the iboss on your network. You can access the iboss interface from any computer on the local network by opening a Web Browser and typing the IP address of the iboss into your Web Browser’s address bar.

Please refer to the iboss SWG Web Filter Deployment Guide for other deployment options.

7 Threat Console

This section allows you to configure how the SWG will log and report traffic flowing through it. You can configure the device to have onboard reporter to report to an external reporter.

7.1 Report Settings

7.1.1 General Settings

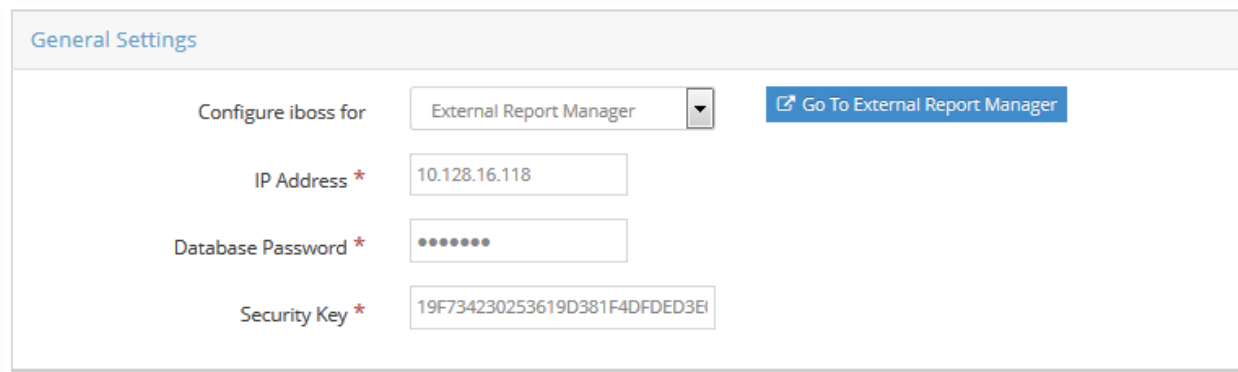


Figure 57 – Report Settings – General Settings

Configure iboss for – You may choose between Onboard Reporting and External Report Manager. If you have an External Report Manager, please choose External Report manager and refer to the following fields.

NOTE

This feature is only available with the Enterprise Reporter Appliance.

IP Address – Enter the IP address of the External Report Manager

Database Password – Enter the database password setup for the reporter. Default is ibossdb.

Security Key – Enter the security key from your reporter after adding it as a registered gateway.

7.1.2 Log Web Statistics

Log Web Statistics

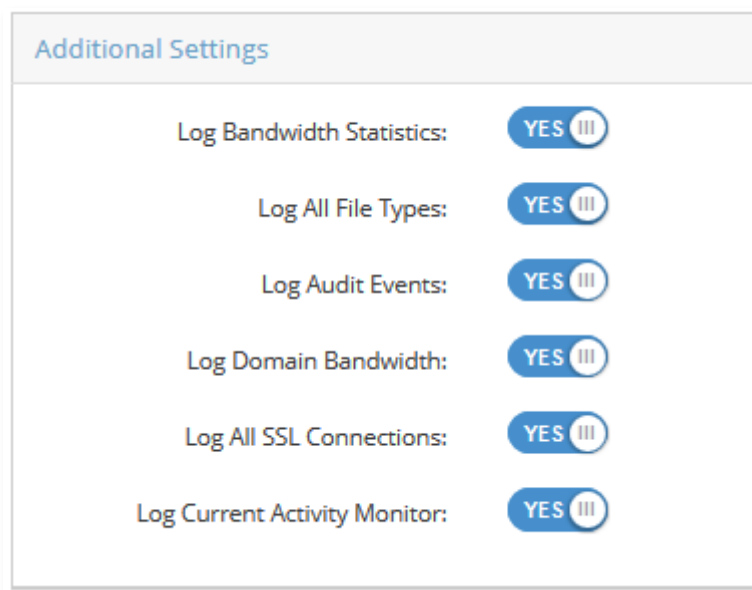
Turn Logging on ☒

Ads <input checked="" type="checkbox"/>	Adult Content <input checked="" type="checkbox"/>	Alcohol & Tobacco <input checked="" type="checkbox"/>	Art <input checked="" type="checkbox"/>
Auctions <input checked="" type="checkbox"/>	Audio & Video <input checked="" type="checkbox"/>	Business <input checked="" type="checkbox"/>	Dating & Personals <input checked="" type="checkbox"/>
Dictionary <input checked="" type="checkbox"/>	Drugs <input checked="" type="checkbox"/>	Education <input checked="" type="checkbox"/>	Entertainment <input checked="" type="checkbox"/>
File Sharing <input checked="" type="checkbox"/>	Finance <input checked="" type="checkbox"/>	Food <input checked="" type="checkbox"/>	Forums <input checked="" type="checkbox"/>
Friendship <input checked="" type="checkbox"/>	Gambling <input checked="" type="checkbox"/>	Games <input checked="" type="checkbox"/>	Government <input checked="" type="checkbox"/>
Guns & Weapons <input checked="" type="checkbox"/>	Health <input checked="" type="checkbox"/>	Image / Video Search <input checked="" type="checkbox"/>	Jobs <input checked="" type="checkbox"/>
Mobile Phones <input checked="" type="checkbox"/>	News <input checked="" type="checkbox"/>	Organizations <input checked="" type="checkbox"/>	Political <input checked="" type="checkbox"/>
Porn - Child <input checked="" type="checkbox"/>	Porn/Nudity <input checked="" type="checkbox"/>	Private Websites <input checked="" type="checkbox"/>	Professional Services <input checked="" type="checkbox"/>
Real Estate <input checked="" type="checkbox"/>	Religion <input checked="" type="checkbox"/>	Search Engines <input checked="" type="checkbox"/>	Sex Ed <input checked="" type="checkbox"/>
Shopping <input checked="" type="checkbox"/>	Sports <input checked="" type="checkbox"/>	Streaming Radio/TV <input checked="" type="checkbox"/>	Swimsuit <input checked="" type="checkbox"/>
Technology <input checked="" type="checkbox"/>	Toolbars <input checked="" type="checkbox"/>	Transportation <input checked="" type="checkbox"/>	Travel <input checked="" type="checkbox"/>
Violence & Hate <input checked="" type="checkbox"/>	Warez <input checked="" type="checkbox"/>	Web Hosting <input checked="" type="checkbox"/>	Web Proxies <input checked="" type="checkbox"/>
Webmail <input checked="" type="checkbox"/>			

Figure 58 – Report Settings – Log Web Statistics

This allows you to enable or disable logging for web statistics. You may choose from the different categories to log.

7.1.3 Additional Settings



Additional Settings	
Log Bandwidth Statistics:	YES III
Log All File Types:	YES III
Log Audit Events:	YES III
Log Domain Bandwidth:	YES III
Log All SSL Connections:	YES III
Log Current Activity Monitor:	YES III

Figure 59 – Report Settings – Additional Settings

Log Bandwidth Statistics – This allows you to enable or disable logging bandwidth statistics.

Log All File Types – This allows you to enable or disable logging of all file types. By default, this is disabled for images, and resources on the page may not be logged in the URL Log.

Log Auditing Events – This allows you to enable or disable logging of auditing events. These are changes that are made in the controls of the iboss by delegated administrators. You can go to the Logs section of the reporter and change the “Audit Only” field to “Yes” allowing you to see all changes made to the configuration of the iboss, and by whom.

Log Domain Bandwidth – This allows you to enable or disable the logging of bandwidth per domain for statistics. This is disabled by default for faster performance.

Log All SSL Connections – This allows you to enable or disable logging for SSL connections.

Log Current Activity Monitor – This allows you to enable or disable the current activity monitor.

7.2 URL Pattern Ignore List

URL Pattern Ignore List

URL Patterns

Delete Selected...

Filter...

<input type="checkbox"/>	URL Pattern	Actions
<input type="checkbox"/>	facebook.com/plugins	<input type="button" value="Remove"/>
<input type="checkbox"/>	connect.facebook.net	<input type="button" value="Remove"/>
<input type="checkbox"/>	commons.wikimedia.org/w/api.php	<input type="button" value="Remove"/>
<input type="checkbox"/>	api.flickr.com/services	<input type="button" value="Remove"/>
<input type="checkbox"/>	en.wikipedia.org/w/api.php	<input type="button" value="Remove"/>
<input type="checkbox"/>	api.twitter.com	<input type="button" value="Remove"/>
<input type="checkbox"/>	platform.twitter.com/widgets	<input type="button" value="Remove"/>
<input type="checkbox"/>	apps-apis.google.com	<input type="button" value="Remove"/>
<input type="checkbox"/>	api.linkedin.com	<input type="button" value="Remove"/>
<input type="checkbox"/>	services.digg.com	<input type="button" value="Remove"/>
<input type="checkbox"/>	api.bing.com	<input type="button" value="Remove"/>
<input type="checkbox"/>	facebook.com/extern/login_status.php	<input type="button" value="Remove"/>

Figure 60 – Report Settings – URL Pattern Ignore List

This page allows you to add domains which you do not wish to log to the iboss Reports database. Domains in the list will be ignored from logging, however all filtering policies will still apply. This is useful for preventing the logging of sites like antivirus updates, operating system updates, etc.

Enter the domain or sub-domain of the website you would like to exclude from being logged to the iboss Reports database. Enter the domain in the text box below and click the **"Add"** button. To remove a website domain from the Ignore List, select the domain and click the **"Remove"** button located at the bottom of the page. When you are finished, click the **"Done"** button.

7.3 Reporter

This section brings you to the web interface of the Threat & Event Console. Please refer to the Threat Console Manual for more information.

8 Configure Controls

The "**Configure Controls**" menu lets you choose options for configuring the current iboss Internet controls.

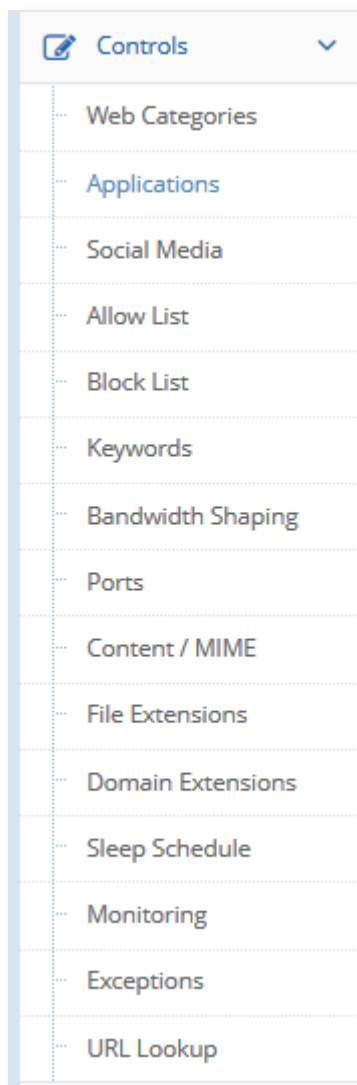


Figure 61 – Configure Internet Controls Menu

Web/SSL Categories – This section allows you to block or allow website content based on categories.

Applications Management – This section allows you to configure access to web applications that the iboss can manage. You may choose to block Chat (Instant messenger) programs, File Sharing programs, FTP & other protocols for Data Leakage Protection (DLP).

Advanced Social Media & Web 2.0 Controls – This section allows you to configure some of the social media sites and other web 2.0 sites like advanced Google and YouTube features. Another feature includes

Pinterest Controls. In addition, using the Local SSL Inspection Agent or Gateway SSL Decryption, other controls appear that can be used for social media sites such as Facebook, Twitter, and LinkedIn as well as more advanced Google controls.

Allow List – This section allows you to permit access to specific websites by adding them to the Allow List.

Block List – This section allows you to block access to specific websites by adding them to the Block List.

Keyword Blocklist/Allowlist – This section allows you to block specific keywords from searches or full URL's by adding them to the Keyword list.

Bandwidth Shaping – This section allows you to set bandwidth restrictions/limits & reservations on users, groups, domains, or web categories. Additional modules allow you to setup bandwidth pools for parent and child rules.

Port Blocking – This section allows you to block specific ports or port ranges with Protocol and Direction.

Content/MIME Type Restrictions – This section allows you to block specific content types and MIME types from being downloaded through the web.

File Extension Blocking – This section allows you to block specific file extensions from being downloaded on your network.

Domain Extension Restrictions – This section allows you to block or allow specific domain extensions from being accessed.

Sleep Schedule – This section allows you to schedule access to the Internet on a schedule.

Real-time Monitoring/Recording – This section allows you to set notification alerts for real-time monitoring and recording when thresholds are met.

Exception Requests – If enabled, a link on the block page will allow users to request the page be allowed. The requests are managed from this page.

URL Lookup – URLs can be searched here to determine how they are categorized. You can also submit a site for re-categorization.

8.1.1 Web / SSL Categories

The 'Categories' window shows a grid of categories. Each category has a set of icons for configuration (up/down arrows, lock, etc.) and a 'Priority' input field. The categories are organized into two columns. The left column includes: Streaming Radio/TV, Porn/Nudity, Dictionary, Drugs, Finance, Gambling, Education, Mobile Phones, Private Websites, Shopping, Travel, Warez, and Known Category. The right column includes: Ads, Audio & Video, Dating & Personals, Entertainment, Forums, Games, Jobs, News, Web Proxies, Sports, Violence & Hate, Webmail, and Guns & Weapons. Each category's 'Priority' field is currently set to 0.

Figure 62 – Web/SSL Categories

The 'Web/SSL Categories' page allows you to configure the current iboss Internet website category blocking settings, log settings, Stealth Mode, and Identity Theft Detection options.

8.1.1.1 Category Scheduling

The 'Advanced Scheduling for Filtering Categories' dialog box contains the following elements:
- A 'Group' dropdown menu currently showing 'Group 1'.
- A warning message: 'For the Advanced Category Scheduling to function, the category to be scheduled must be currently blocked.'
- An 'Apply Schedule To All Categories' toggle set to 'YES'.
- An 'Apply Schedule To' dropdown set to 'Specific Day (below)'.
- A calendar view showing days of the week (Monday to Sunday). A green bar is visible on Monday, indicating a scheduled time range from 2:00 AM to 5:00 PM.
- Action buttons at the bottom: 'Clear Schedule', 'Close', and 'Save'.

Figure 63 – Category Scheduling

You may use advanced scheduling to create custom allow and block times for Filtering Categories. You may use different schedules for the different days of the week by selecting the day and setting the schedule. For Filtering Categories you will have to select a Category to Schedule:

Green (or checked) indicates access is allowed during the time block specified.

Red (or unchecked) indicates access is blocked during the time block specified.

Note: For the Advanced Category Scheduling to function, the category to be scheduled must be currently blocked on the "**Internet Category Blocking**" setup page.

8.1.1.2 Additional Settings

Additional Settings

Enable Logging	<input checked="" type="checkbox"/>	Enable Stealth Mode	<input type="checkbox"/>	Enable Strict SafeSearch Enforcement	<input type="checkbox"/>
Enable HTTP Scanning on non-standard ports	<input checked="" type="checkbox"/>	Allow Legacy HTTP 1.0 requests	<input checked="" type="checkbox"/>	Enable ID Theft / IP Address URL Blocking	<input type="checkbox"/>

Enable Logging – Allows you to enable and disable logging of violation attempts for the current set of blocked website categories. Log reports may be viewed on the iboss Reports page. The report information includes date, time, user, website address, and category of the violation.

Enable Stealth Mode – Allows you to stealthily monitor Internet activity without blocking access to forbidden sites. With both Logging and Stealth Mode enabled, you can monitor Internet web surfing activity by viewing the log reports on the iboss Reports page while remaining unnoticed to Internet users on the network.

NOTE	Websites and online applications will not be blocked while the iboss is in "Stealth Mode."
-------------	--

NOTE	Enable Strict SafeSearch Enforcement – Allows you to enforce strict safe search preferences on Google, Yahoo, YouTube and Bing search engines. This includes image searching. If this option is enabled and the user does not have search engine preferences set to strict safe searching, the iboss will automatically change the user's preferences to strict safe searching before performing the search. This allows an extra layer of enforcement to prevent unwanted adult and explicit content from being searched for on these search engines.
-------------	---

Enable HTTP Scanning on Non-Standard Ports – If this feature is enabled, the iboss will scan for HTTP web requests on non-standard ports.

Allow Legacy HTTP 1.0 Requests – If this feature is enabled, the iboss will allow HTTP 1.0 requests that are missing the "HOST" header. Disabling this feature provides a higher level of filtering security and makes

bypassing the filter more difficult. If this feature is enabled, it may provide more compatibility with older non HTTP 1.1 compliant software.

Enable ID Theft / IP Address URL Blocking – Protects against potential identity theft attempts by notifying you when someone is trying to steal your personal information through Internet Phishing. Enabling this feature will also block users from navigating to websites using IP address URL's.

8.1.1.3 Categories

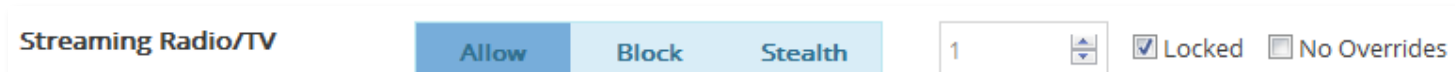


Figure 64 – Category Example

These are categories in which Internet websites are grouped. You may choose categories from this list that you wish to block on your network. In addition to blocking access to these website categories, the iboss will also log attempted access violations if logging is enabled.

Examples of website categories are:

Ads	Forums	Private Websites
Adult Content	Friendship	Real Estate
Alcohol/Tobacco	Gambling	Religion
Art	Games	Restaurants/Food
Auctions	Government	Search Engines
Audio & Video	Guns & Weapons	Services
Bikini/Swimsuit	Health	Sex Ed
Business	Image/Video Search	Shopping
Dating & Personals	Jobs	Sports
Dictionary	Mobile Phones	Streaming Radio/TV
Drugs	News	Technology
Education	Organizations	Toolbars
Entertainment	Political	Transportation
File Sharing	Porn/Nudity	Travel
Finance & Investment	Porn – Child	Violence & Hate

Virus & Malware

Web Hosting

Web-Based E-mail

Web Proxies

Allow/Block/Stealth – Specifies whether the category is blocked or allowed for this filtering group. Designating 'Stealth' will flag as a violation but will not actually block.

Priority – By default 'Block' has priority over 'Allow'. A site belonging to multiple categories will be blocked if ANY of those categories are blocked unless a category with a higher priority is allowed. For example: A site belonging to both 'Education' and 'gaming' would be blocked if the policy is to block all gaming. If 'Education' priority is bumped to 1 (or anything higher than that of gaming) then the site is allowed.

Locked – A Delegated Administrator will not be able to alter the category settings of those flagged as 'Locked'.

No Override – A Delegated Administrator will not be able to add URLs to the Allow list if they belong to a banned category marked as 'No Override'.

8.1.1.4 Identify Theft (Phishing)/ IP Address Blocking Page

When a page is blocked from of the iboss due to detection of Identity Theft (Phishing)/IP

Address URL Blocking, this page will show up in the web browser to the user. You may manually login and add the blocked Identity theft page (IP address) to the allow list if you feel that you have received the Identity Theft Detection in error by typing in the password and pressing Login.

8.1.2 Application Management

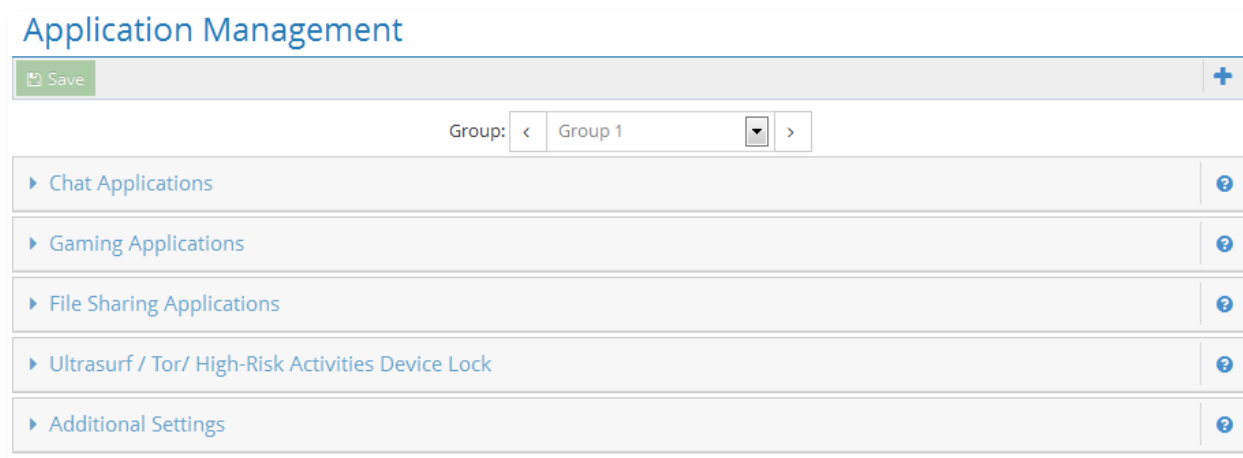


Figure 65 – Application Management

The "Application Management" section allows you to configure the current iboss program blocking settings.

8.1.2.1 Chat Applications

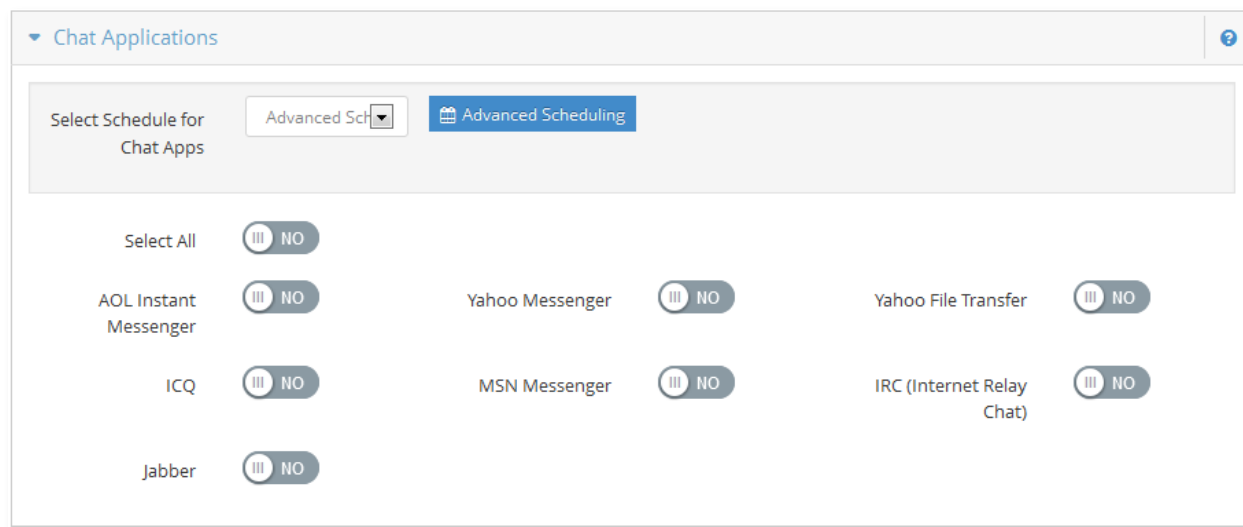


Figure 66 – Applications – Chat Applications

This category contains applications used for online messaging and chat. The iboss can block the selected program(s) and log attempted violations. Examples of applications in this category are:

AIM (AOL Instant Messenger)

MSN Messenger

Yahoo Messenger/Yahoo File Transfer

IRC (Internet Relay Chat)

ICQ

Jabber

Advanced Scheduling – Allows you to schedule daily access for selected chat programs. This option will bypass blocking for chat and instant messenger programs during the specified time.

8.1.2.2 Gaming Applications

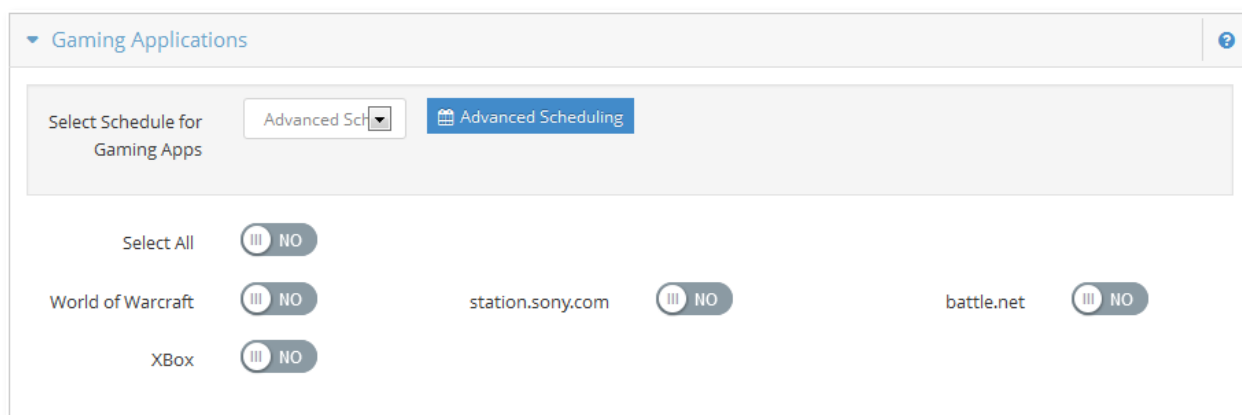


Figure 67 – Applications – Gaming Applications

This category contains online gaming applications. The iboss can block the selected program(s) and log attempted access violations. Examples of applications in this category are:

World of Warcraft

Battle.net

StarCraft

XBox

Station.sony.com

Advanced Schedule – Allows you to schedule daily access for selected online gaming programs. This option will bypass blocking for online gaming programs during the specified time.

8.1.2.3 File Sharing Applications

Figure 68 – Applications – File Sharing Applications

This category contains online file sharing applications. The iboss can block the selected program(s) and log attempted access violations. Examples of applications in this category are:

LimeWire

Acquisition

Ares

XoloX

BitTorrent

Direct Connect

ZP2P

Edonkey

BearShare

Manolito

Advanced Scheduling – Allows you to schedule daily access for selected file sharing programs. This option will bypass blocking for file sharing programs during the specified time.

8.1.2.4 Ultrasurf / Tor / High–Risk Activity Device Lock

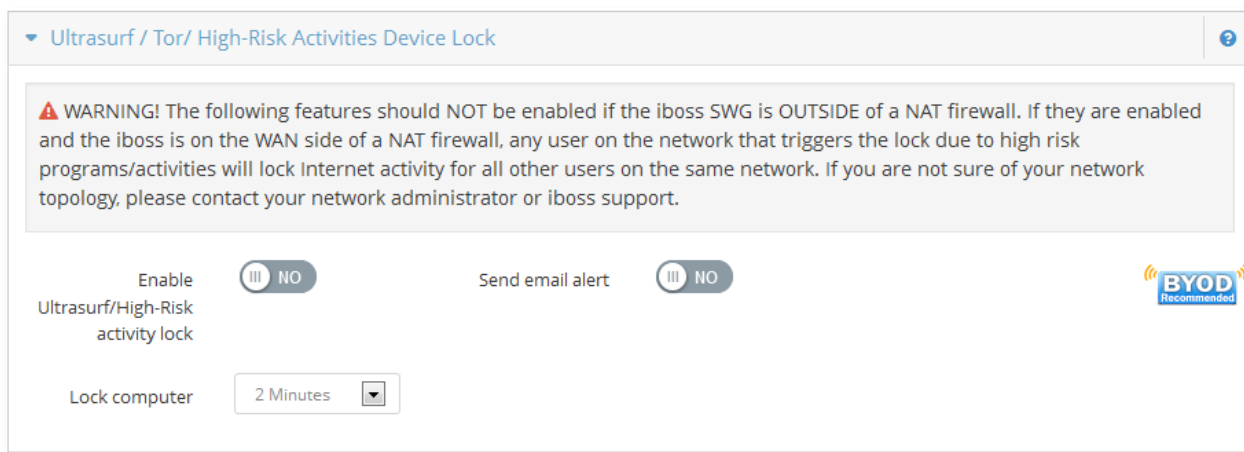


Figure 69 – Ultrasurf / Tor / High–Risk Activity Device Lock

Enable Ultrasurf/High–Risk activity lock – This feature blocks the use of Hotspot Shield, OpenVPN, Spotflux, and Expat Shield. It also allows you to lock the Internet for a user if the use of Ultrasurf/Tor Proxies is detected. This blocks all Internet access so that when the user opens a web browser, they will be informed that the detection has occurred and that they must disable the program. The Internet will be blocked for the specified time.

Send email alert – This option will inform the iboss administrator that the detection has occurred when the event is detected. By default, it will email the address setup for the User Alerts (Reporter → Registered Devices). The individual filtering group can have a group email contact under Controls → Monitoring. The email address listed in the Monitoring section, for any given group, will override the master alerts email address listed in the Reporter.

Lock computer – When Ultrasurf/high–risk activity is detected allows you to specify an amount of time in minutes that the user would be locked for. This will lock the computer from going to the Internet from the time it has detected this event for the amount of minutes that you specify. The suggested setting for this value is 5 minutes, but you can set a lower or higher value.

You can unlock a computer manually by finding the computer under the Groups→ Computers tab and click Unlock.

WARNING! These features should NOT be enabled if the iboss SWG is OUTSIDE of a NAT firewall. If they are enabled and the iboss is on the WAN side of a NAT firewall, any user on the network that triggers the lock due to high risk programs/activities will lock Internet activity for all other users on the same network. If you are not sure of your network topology, please contact your network administrator or iboss support.

8.1.2.5 Additional Settings

Additional Settings		
Block SSH / Secure Shell Access	<input type="radio"/> NO	
Block RDP/ Remote Desktop Access	<input type="radio"/> NO	
Block Incoming FTP Traffic	<input checked="" type="radio"/> YES	
Block Outgoing FTP Traffic	<input checked="" type="radio"/> YES	
Block Ping (ICMP)	<input type="radio"/> NO	
Dynamic Proxy Blocking(Glyphe)	<input type="radio"/> NO	
Block Hotspot Shield	<input type="radio"/> NO	
Block SSL on Non-standard Ports	<input type="radio"/> NO	
Block Rogue Encrypted Connections	<input type="radio"/> NO	
SSL Domain Enforcement	<input type="radio"/> NO	
Reverse DNS Lookup Support	<input checked="" type="radio"/> YES	
Block Newsgroups	<input type="radio"/> NO	
Block Internal Servers	Disabled	
Logging	<input checked="" type="radio"/> YES	

Figure 70 – Application – Additional Settings

Block SSH/Secure Shell Access – You may choose block incoming and outgoing SSH Shell Access.

Block RDP/Remote Desktop Access – You may choose to block incoming and outgoing Remote Desktop Access.

Block Incoming FTP Traffic – You may choose to block incoming FTP Traffic.

Block Outgoing FTP Traffic – You may choose to block outgoing FTP Traffic.

Block Ping (ICMP) – You may choose to block outgoing Ping (ICMP) Traffic.

Dynamic Proxy Blocking (Glype) – You may choose to block dynamic Glype-themed proxy sites. These are proxy sites setup using the Glype Proxy script which the iboss can detect and block dynamically regardless of the domain.

Block Hotspot Shield – You may choose to block Hot Spot Shield. Hot Spot Shield is a program used to proxy to Hot Spot Shields servers. Enabling this feature will block the program from being used as a proxy.

Block SSL on Non-Standard Ports – You may choose to enable blocking SSL on Non-Standard Ports. This feature is useful for blocking File Sharing programs which use encryption over non-standard ports.

Block Rogue Encrypted Connections – You may choose to enable blocking for Rogue Encrypted Connections. This option blocks invalid SSL certificates and blocks programs that use Rogue Encryptions such as UltraSurf.

SSL Domain Enforcement – This option validates domains with the SSL certificate.

Reverse DNS Lookup Support – This option allows for Reverse DNS lookup support, tracing an IP back to the domain it belongs to.

Block Newsgroups – You may choose to block newsgroup traffic.

Block Internal Servers – You may choose to enable blocking for internal Servers. This option helps block programs like BitTorrent which upload as well as download.

Logging – Allows you to enable or disable logging of attempted program access violations. This log is found on the Reports page. The logging includes date, time, and category. Logging can be enabled while in stealth mode. This is useful for monitoring your Internet usage while remaining unnoticed on the network. Without logging, the iboss program blocking will still work however violations will not be logged.

8.1.3 Advanced Social Media & Web 2.0 Controls

Figure 71 – Advanced Social Media & Web 2.0 Controls

8.1.3.1 Social Chat App Controls

Figure 72 – Social Chat App Controls

This feature allows you to block the Snapchat application on mobile devices.

8.1.3.2 Social Streaming Radio Controls

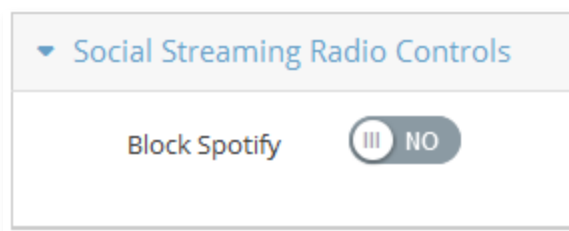


Figure 73 – Social Streaming Radio Controls

This feature allows you to block Spotify.

8.1.3.3 Pinterest Controls

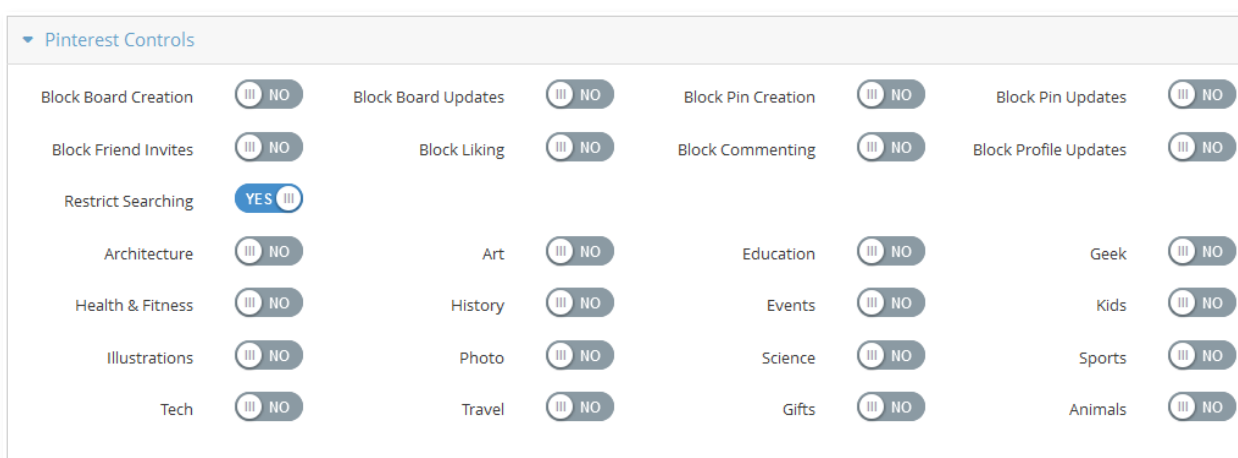


Figure 74 – Pinterest Controls

These features allow you to configure particular sections of Pinterest websites. The following options are available to choose to block:

- Block Board Creation
- Block Board Updates
- Block Pin Creation
- Block Pin Updates
- Block Friend Invites
- Block Liking
- Block Commenting
- Block Profile Updates

■ Restrict Searching to selected categories:

- Architecture
- Art
- Education
- Geek
- Health & Fitness
- History
- Events
- Kids
- Illustrations
- Photo
- Science
- Sports
- Tech
- Travel Gifts
- Animals

8.1.3.4 Facebook Controls

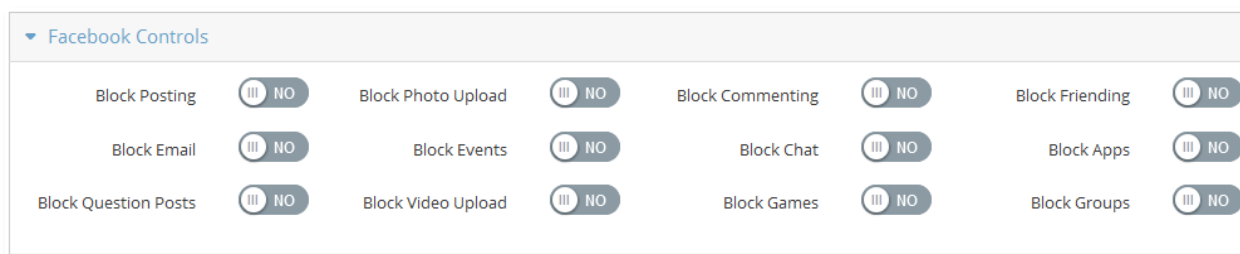


Figure 75 – Facebook Controls

SSL Decryption for facebook.com needed – These features allow you to block specific features and sections for facebook.com. The following options are available to choose to block:

- | | |
|----------------------|------------------------|
| ■ Block Posting | ■ Block Chat |
| ■ Block Photo Upload | ■ Block Apps |
| ■ Block Commenting | ■ Block Question Posts |
| ■ Block Friending | ■ Block Video Upload |
| ■ Block Email | ■ Block Games |
| ■ Block Events | ■ Block Groups |

8.1.3.5 Twitter Controls

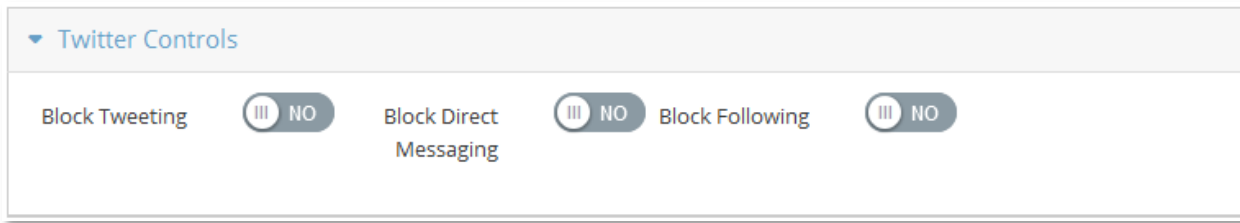


Figure 76 – Twitter Controls

SSL Decryption for twitter.com needed – These features allow you to block specific features and sections for twitter.com. The following options are available to choose to block:

- ☐ Block Tweeting
- ☐ Block Direct Messaging
- ☐ Block Following

8.1.3.6 Linked-in Controls

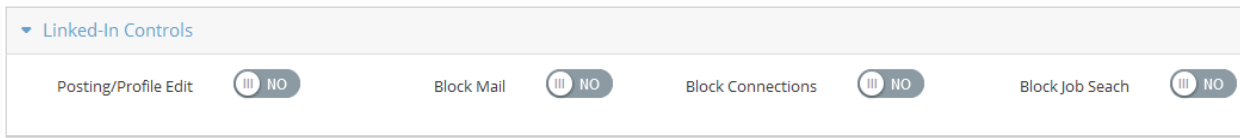
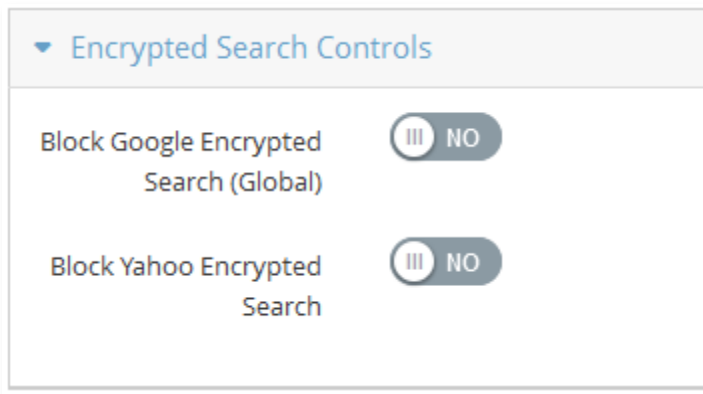


Figure 77 – Linked-in Controls

SSL Inspection Agent needed – These features allow you to block specific features and sections for linkedin.com. The following options are available to choose to block:

- ☐ Block Posting/Profile Edit
- ☐ Block Mail
- ☐ Block Connections
- ☐ Block Job Search

8.1.3.7 Encrypted Search Controls



▼ Encrypted Search Controls

Block Google Encrypted Search (Global) ☐ NO

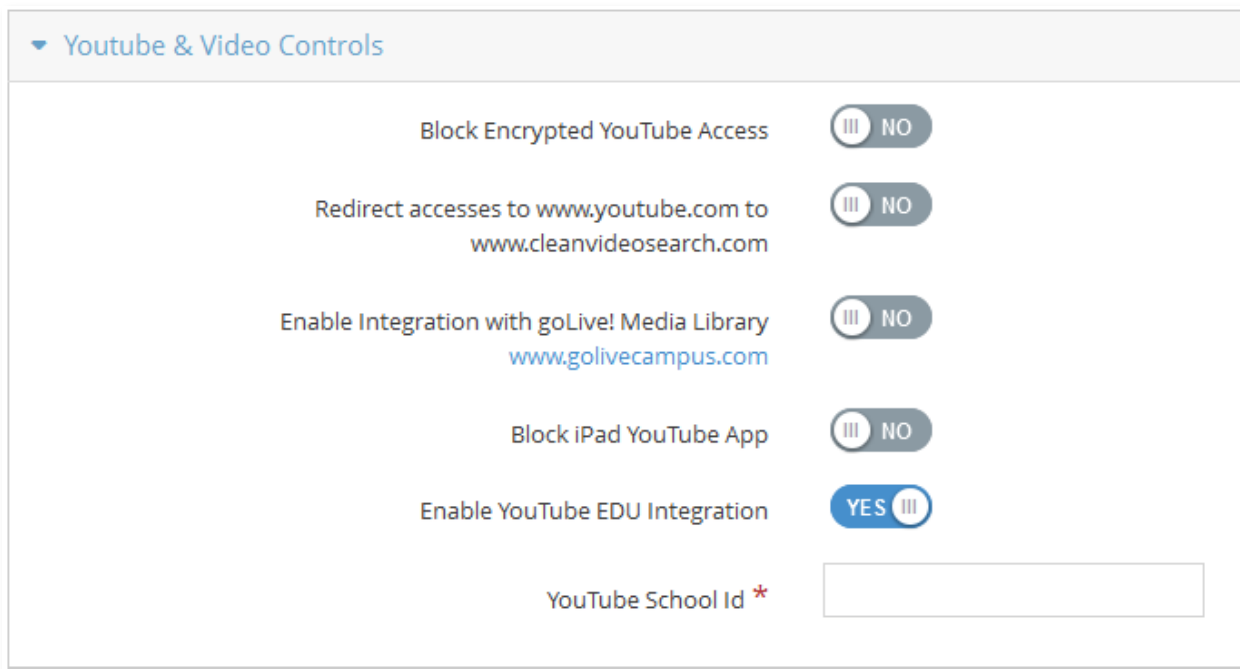
Block Yahoo Encrypted Search ☐ NO

Figure 78 – Encrypted Search Controls

Block Google Encrypted Search (Global) – Allows for automatic redirections to unencrypted search pages.

Block Yahoo Encrypted Search – Allows for blocking of Encrypted Yahoo Searches. HTTP requests for yahoo.com get directed to an non-encrypted search page.

8.1.3.8 YouTube & Video Controls



▼ Youtube & Video Controls

Block Encrypted YouTube Access ☐ NO

Redirect accesses to www.youtube.com to www.cleanvideosearch.com ☐ NO

Enable Integration with goLive! Media Library www.golivecampus.com ☐ NO

Block iPad YouTube App ☐ NO

Enable YouTube EDU Integration ☒ YES

YouTube School Id *

Figure 79 – YouTube & Video Controls

These features allow you to controls certain features of YouTube as well as handle requests to YouTube differently for specific filtering groups.

Block Encrypted YouTube Access – This option will block encrypted https access to YouTube (now on a per-group basis). If your DNS server has direct access to the Internet without going to through the iboss or you have

the iboss in tap mode, you would want to setup a DNS Conditional Forwarder for youtube.com to point to the iboss. You can get these instructions from iboss support.

Redirect accesses to www.youtube.com to www.cleanvideosearch.com – This redirects any request to youtube.com to cleanvideosearch.com. Cleanvideosearch.com is a site that provides searching for videos from YouTube.com while enforcing Strict Safety Mode and stripping out all comments and related videos. You can set this option on a per group basis.

Enable Integration with goLive! Media Library www.golivecampus.com – This feature allows you to block YouTube.com but allow videos to be played from golivecampus.com. Golivecampus.com is a site that allows you to granularly choose which videos are allowed to be viewed with channels that can have videos linked on them.

Block iPad YouTube App – This option allows you to block the YouTube App on mobile devices.

Enable YouTube EDU integration – This feature integrates with YouTube for Schools. This allows you to enter your **YouTube School ID** and this will be appended to each request to YouTube allowing only educational videos from YouTube to be allowed to play.

8.1.3.9 Google Controls

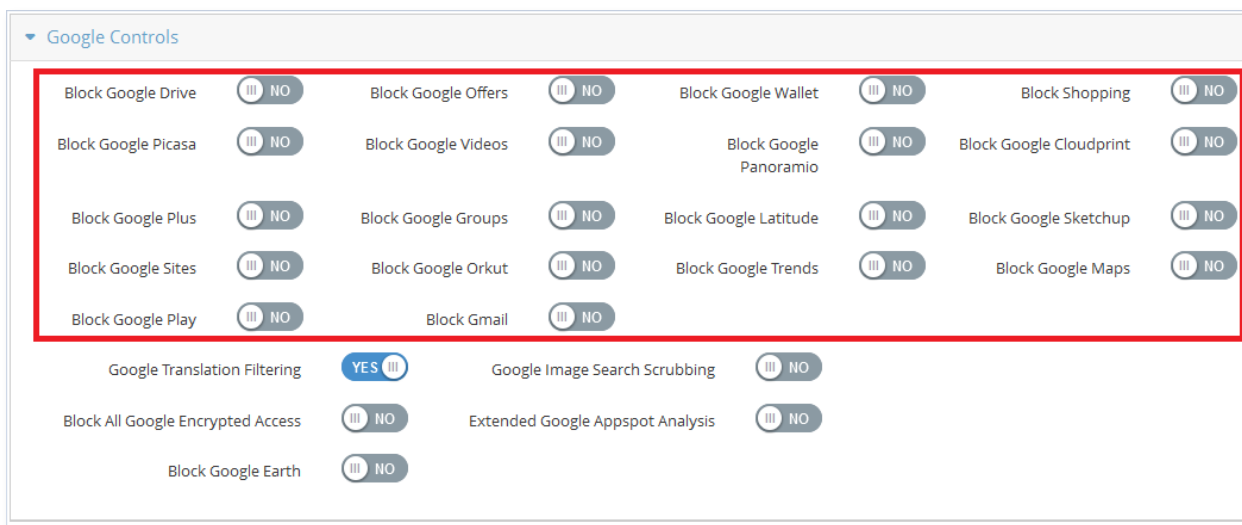


Figure 80 – Google Controls

Features in the red box above need SSL Decryption – These features from Google in allow you to control specific sections of Google by decrypting and enabling these features.

Google features that are available when enabling the SSL inspection Agent/Enabling Gateway Decryption are:

- Block Google Drive
- Block Google Offers
- Block Google Wallet
- Block Shopping
- Block Google Groups
- Block Google Latitude
- Block Google SketchUp
- Block Google Sites
- Block Google Orkut
- Block Google Trends
- Block Google Maps

- Block Google Picasa
- Block Google Videos
- Block Google Panoramio
- Block Google Cloudprint
- Block Google Plus

Google Translation Filtering – This feature blocks violation sites from being translated using Google Translation.

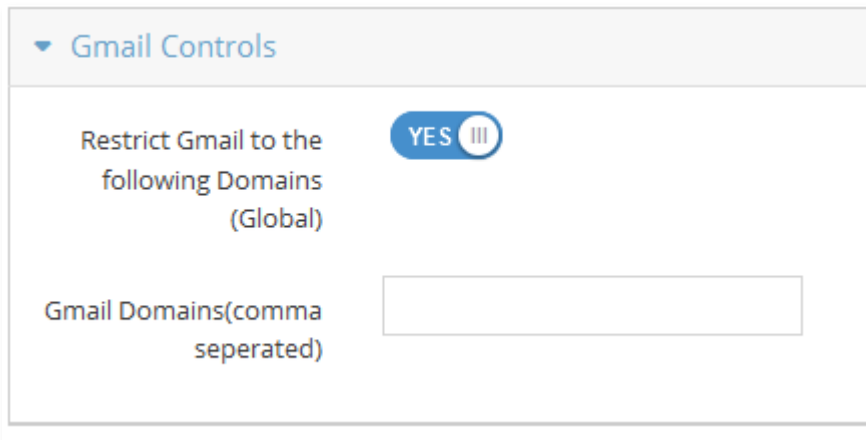
Google Image Search Scrubbing – This feature strips out images on Google Image Searches that come from violation sites that are block by the categories.

Block All Google Encrypted Access – This feature blocks all encrypted Google services.

Extended Google Appspot Analysis – This feature lets you allow access to appspot.com but block subdomains of appspot.com based on DNS.

Block Google Earth – This feature blocks Google Earth.

8.1.3.10 Gmail Controls



▼ Gmail Controls

Restrict Gmail to the following Domains (Global) YES III

Gmail Domains(comma seperated)

Figure 81 – Gmail Controls

Restrict Gmail to the following Domains (Global) – This features allows you to restrict Gmail access to only the domains you specify.

8.1.4 Allowlist

Allowlist

Group: < Group 1 >

Preferences

☐ ONLY ALLOW access to sites on the Allowlist below

[Save](#)

Custom Category Assignments

Custom Categories

- Students Allow1
- Custom Category 2
- Custom 5
- Custom 6

>>

<<

Chosen Categories

- Video Sites
- Custom 4
- Custom 10

[Save](#) [Manage Categories](#)

Allowlist

☐ Global
 ☐ SafeSearch
 [+Add](#)

[Delete Selected...](#)
[+Import...](#)

<input type="checkbox"/>	Url	Timeout	Global	Safe Search	Actions
<input type="checkbox"/>	ibk.com	N/A	No	No	Delete
<input type="checkbox"/>	booyah.com	N/A	No	No	Delete
<input type="checkbox"/>	rockle.com	N/A	No	No	Delete
<input type="checkbox"/>	lk.com	N/A	No	No	Delete
<input type="checkbox"/>	phil.com	N/A	No	No	Delete
<input type="checkbox"/>	hola.com	N/A	No	No	Delete
<input type="checkbox"/>	beware.com	N/A	No	No	Delete
<input type="checkbox"/>	dang.com	N/A	No	No	Delete
<input type="checkbox"/>	bing.com	N/A	No	No	Delete

Figure 82 – Allowlist

This page allows you to add specific websites to your Allow list. The Allow list is a list of specific Internet URLs that you want to allow on your network. Website URLs added to this list will be allowed even if they are currently blocked in the Web Categories section.

8.1.4.1 Preferences

Allow ONLY access to sites on the Allow list – Checking this option will **only** allow sites on the list.

Alert! If the "Allow ONLY access to sites on the Allow list" option is selected, only the websites in the Allow list below will be allowed. All other websites will be blocked.

Enable Allow list Navigation webpage – This will give you a page that has a list of the allowed sites to be able to give to your users. You may select the "**Enable Allow list Navigation webpage**" if you wish to allow access to a built-in iboss website that will display links to all sites on the Allow list. To apply changes, click the "**Apply**" button.

Note: The Allow list Navigation webpage will only display when the "**Allow ONLY**" feature is enabled.

Default Timed URL Timeout – This is the default setting for when adding sites on this list. By default, sites added to this list will remain until removed. There are options to choose a time limit as a default for removing it after the specified time.

Once you have changed any of these settings, click the "**Save**" button.

8.1.4.2 Allowlist

Enter the URL of the website you would like to allow in the text box below and click the "**Add URL**" button. You may enter a maximum of 1000 website URLs across all profiles. Each URL may be a maximum of 255 characters in length. To remove a website URL from the Allow list, select the URL and click the "**Remove**" button located at the bottom of the page. When you are finished, click the "**Done**" button.

Enter URL (ex: domain.com) – field to enter the domain or URL to allow.

URL Timeout – select how long you would like the URL to remain on the list.

Global – Option to apply rule across all filtering groups

Keyword/Safe Search – if you would still like to have keyword and safe search enforcement applied to the domain being bypassed.

Once you have entered in a URL or domain, click the "**Add**" button.

URL Filter – This feature allows you to search through the list. You can enter part of the domain like Google to see any URLs that are in this list with that word in it. You can click Apply to view entries in this list. To clear the filter, delete the entry in this field and click Apply.

Sorting – You can click on the URL word to sort the list alphabetically.

Removing – Remove a URL by selecting the checkbox next to the URL and click the Remove button at the bottom.

8.1.4.3 Custom Allow list Categories

Allowlist Custom Categories ?

×

Choose Category

Students Allow1 ▾

Category Name *

Students Allow1

YouTube Video Category

YES III

Category Schedule

☐ Always Enabled

☒ Advanced Schedule

Advanced Scheduling

Category Urls ?

Url

SafeSearch

+ Add Url

Delete Selected...

+ Import...

Filter...

<input type="checkbox"/>	Url	Safe Search	Actions
<input type="checkbox"/>	test.com	No	
<input type="checkbox"/>	blah.info	No	
<input type="checkbox"/>	kdjiejifejj.jax	No	
<input type="checkbox"/>	iidudu.inof	No	
<input type="checkbox"/>	hippy.net	No	
<input type="checkbox"/>	ma.com	No	

×

 Close

Save

Figure 83 – Custom Allow list Categories

Select the custom allow list categories to apply to this group. These categories allow you to create custom lists of URLs that can be applied to multiple groups. Use the custom category feature to avoid adding the same URL to multiple groups.

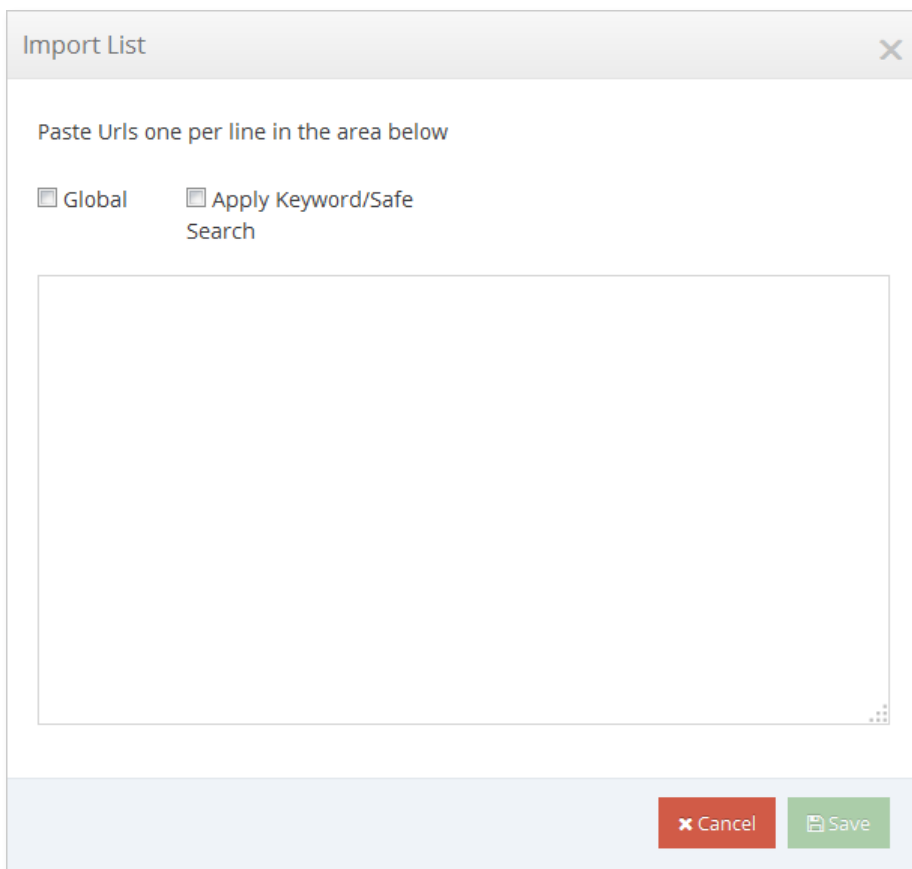
This feature allows you to create custom Allow list categories.

Enter the URL of the website you would like to add in the currently selected category then click the "**Add URL**" button. Any group that has this category checked will have the URLs in this category applied.

YouTube Video Category – This option allows you to allow specific YouTube videos while the Audio/Video category still blocks the YouTube site.

Apply Keyword/Safe Search – Allows the domain or URL, but apply Keyword comparison and Safe Search.

8.1.4.4 Allowlist Import



Import List

Paste Urls one per line in the area below

☐ Global ☐ Apply Keyword/Safe Search

Cancel Save

Figure 84 – Allowlist Import

You may import a list of domains to import. To import on the Allowlist or custom Allowlist, click the **Import** button. Please paste URLs one per line with a maximum of 255 characters per domain/IP/URL. Once you are done, click the "**Save**" button.

8.1.5 Block Specific Websites

Block List

Group: < Group 1 >

Custom Category Assignments

Custom Categories

Custom 1
Custom 2
Custom 3
Custom 4

>>
<<

Chosen Categories

Save Manage Categories

Block List

☐ Global
+ Add

Delete Selected... +Import...

Filter...

<input type="checkbox"/>	Url	Global	Actions
<input type="checkbox"/>	supyall.com	No	<input type="checkbox"/>
<input type="checkbox"/>	yippee.com	No	<input type="checkbox"/>

Figure 85 – Block Specific Websites

This page allows you to block specific website URLs from being accessed on your network.

Enter the URL of the website you would like to block in the text box below and click the **"Add URL"** button. You may enter a maximum of 1000 website URLs across all profiles. Each URL may be a maximum of 255 characters in length. To remove a website URL from the Block list, select the URL to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

8.1.5.1 Custom Block list Categories

Blocklist Custom Categories ?

Choose Category

Custom 1

Category Name *

Custom 1

YouTube Video Category

NO

Category Schedule

☒ Always Enabled
 ☐ Advanced Schedule

Advanced Scheduling

Category Urls

Url

SafeSearch

+Add Url

Delete Selected...

+Import...

Filter...

Url	Safe Search	Actions
hi.com	No	

Close

Save

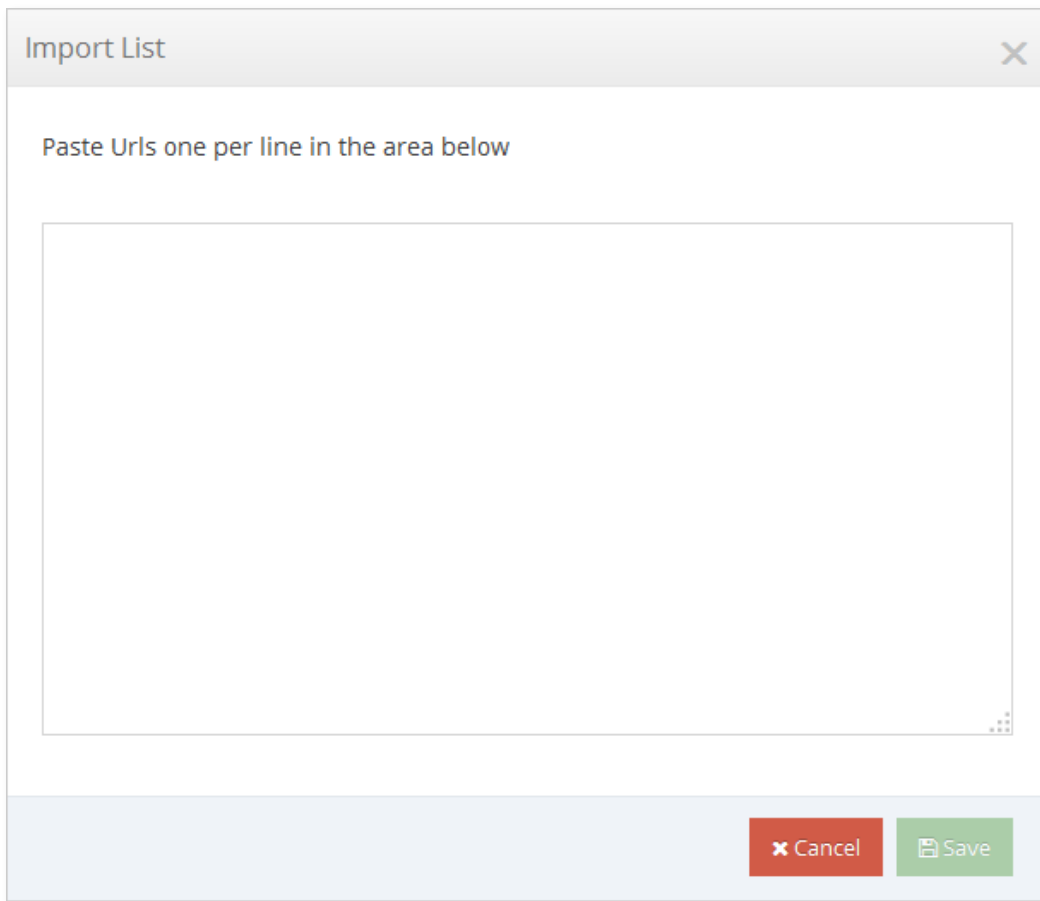
Figure 86 – Custom Block list Categories

Select the custom block list categories to apply to this group. These categories allow you to create custom lists of URLs that can be applied to multiple groups. Use the custom category feature to avoid adding the same URL to multiple groups.

This feature allows you to create custom Block list categories.

Enter the URL of the website you would like to add the currently selected category in the text box below and click the "Add URL" button. Any group that has this category checked will have the URLs in this category applied.

8.1.5.2 Block list Import



Import List

Paste Urls one per line in the area below

Cancel Save

Figure 87 – Block list Import

You may import a list of domains to import. To import, click the **+Import** button. Please paste URLs one per line with a maximum of 255 characters per domain/IP/URL. Once you are done, click the "Import Now" button.

8.1.6 Keyword Blocklist/Allowlist

Keyword Blocklist/Allowlist

Group: < Group 1 >

Pre-defined Keyword Lists

Adult

YES

High Risk

NO

Save

Keywords

Keyword

☐ Allow Keyword
 ☐ Wildcard Match
 ☐ High Risk
 ☐ Global

+Add

Delete Selected...

+Import...

Filter...

Keyword	Allow Keywo...	Wildcard	High Risk	Global	Actions
t1t	No	Yes	No	No	
sexy	No	No	No	No	
naughty	No	No	No	No	

Figure 88 – Keyword Blocklist/Allowlist

This feature allows you to create keyword Block lists. The iboss will block Internet sites that contain these specific keywords in the URL. In addition, web searches using the keywords in the list(s) will also be blocked.

8.1.6.1 Pre-Defined Keyword Lists

You may select from pre-defined keyword category lists. Each category contains its own keyword list. To enable a keyword list, select the checkbox next to the category. You may view and edit the list by clicking on the pencil icon to edit the list. When you are finished, click the **"Save"** button.

High Risk – The words on this list will send the administrator of the group an email notification when searched.

8.1.6.2 Keywords

Enter the custom keyword that you would like to block in the text box below and click the **"Add"** button. You may enter a maximum of 2000 URL keywords across all profiles. Each keyword may be a maximum of 19 characters in length (letters and digits only). To remove a keyword from the list, select the keyword and click the **"Delete Selected"** button located at the bottom of the page.

Allow Keyword – Checking this option will allow the word if it is in the URL within a keyword parameter.

Wildcard Match – Checking this option will use wild card matching on the keyword. When wild card matching is used, the entire URL is searched for the keyword pattern. If wild card matching is not used, the iboss will analyze the URL for queries containing the keyword(s) entered.

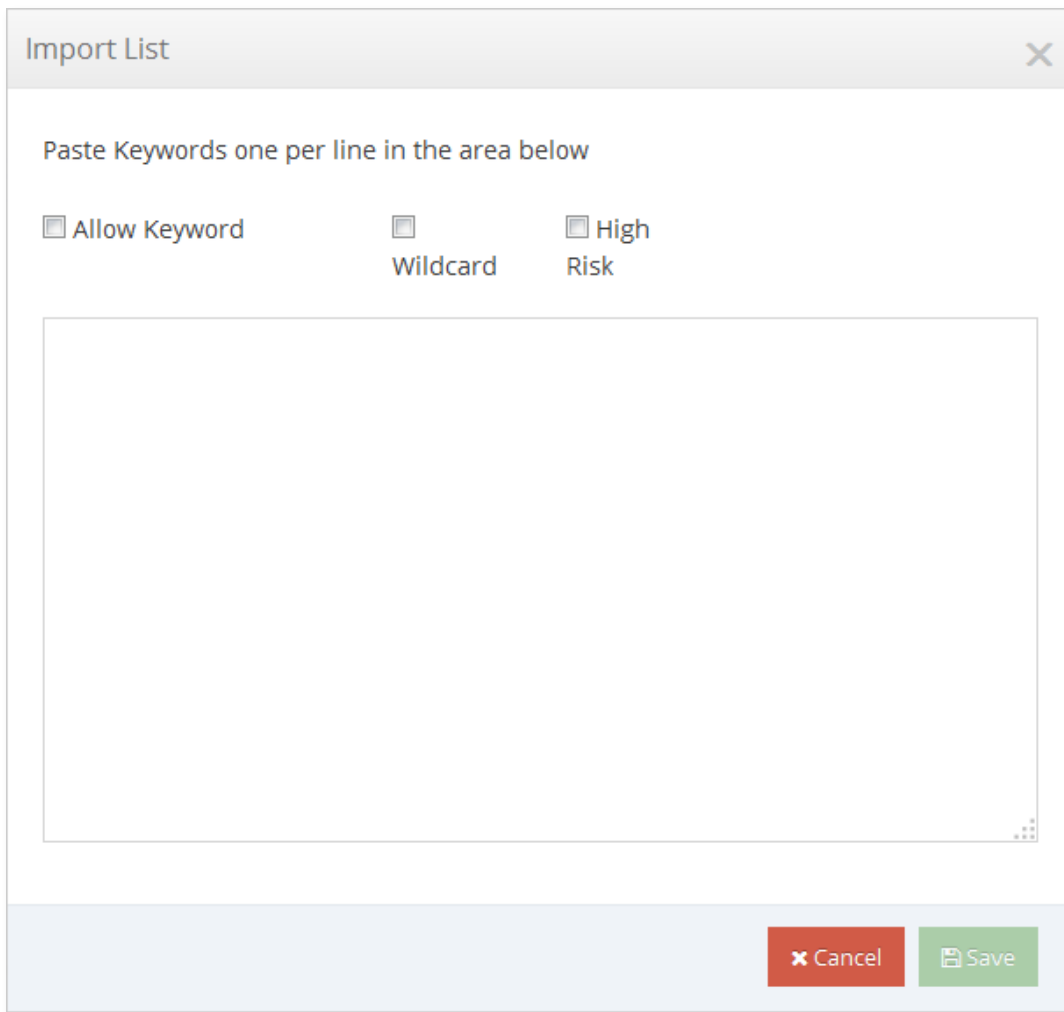
High Risk – This option will send a notification to the group administrator when searched for.

Global – This option will span across all filtering groups when selected. When removing a "Global" entry, it will remove the entry from all filtering groups.

Keyword Searching – You can use the search filter input box to the right to filter the keyword list view.

You can import a list of keywords to block by clicking "**Import**". You may remove keywords by checking the keyword and clicking the "**Delete Selected**" button.

8.1.6.3 Keyword Import



Import List

Paste Keywords one per line in the area below

☐ Allow Keyword ☐ Wildcard ☐ High Risk

Cancel Save

Figure 89 – Keyword Import

You may import a list of keywords to import. Please paste keywords one per line with a maximum of 19 characters per keyword. You may select Allow Keyword, Wildcard, and High Risk when importing. Once you are done, click the **Save** button.

8.1.7 Bandwidth Shaping

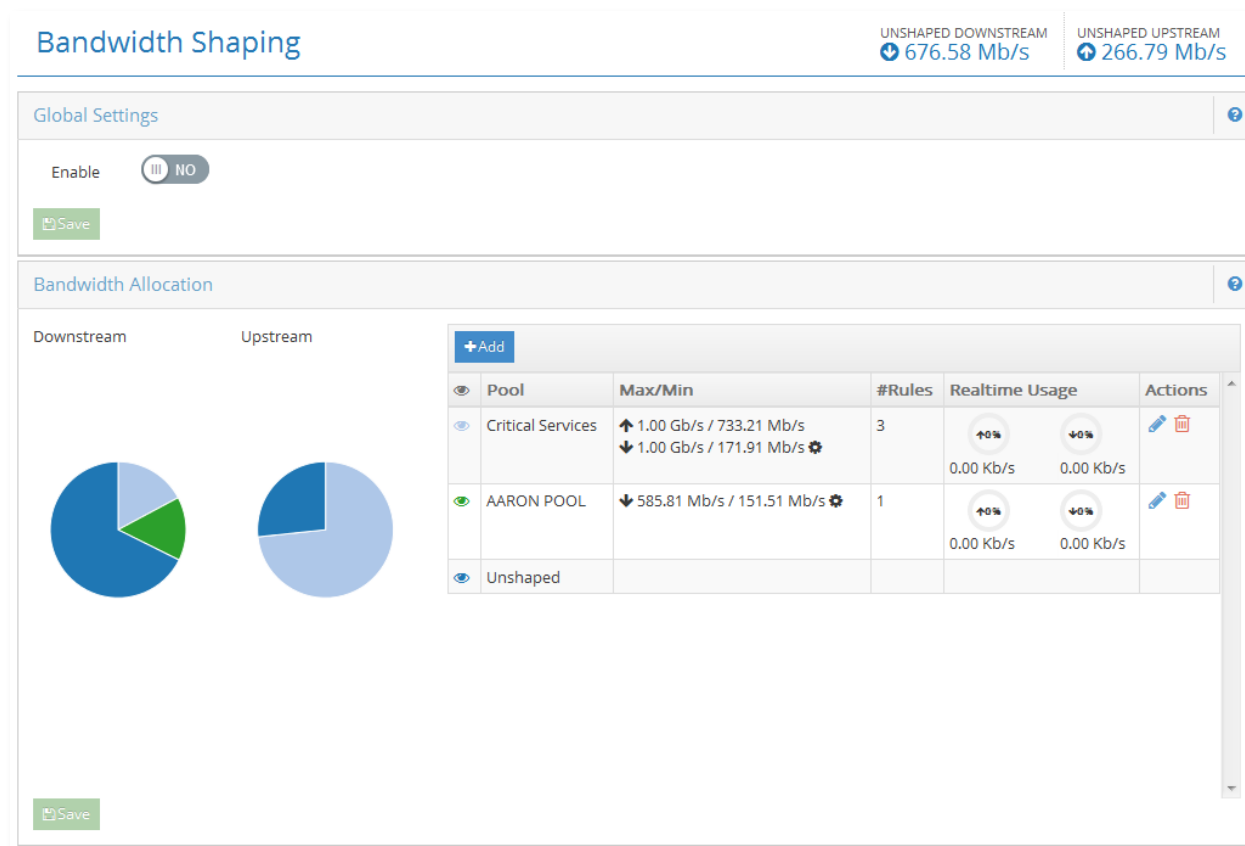


Figure 90 – Bandwidth Throttling

There is a separate, more comprehensive manual for the Bandwidth Throttling/QoS feature. Please request this from iboss Support for the iboss Enhanced QoS & Bandwidth Shaping Datasheet.

8.1.8 Port Blocking

Save

Group: < Group 1 >

Port Blocking Settings

#	Name	Port Start	Port End	Protocol	Direction	Enabled
1	SSH			22	22	Both Tcp Udp Both In Out YES
2	HTTP			80	81	Both Tcp Udp Both In Out YES
3				0	0	Both Tcp Udp Both In Out NO
4				0	0	Both Tcp Udp Both In Out NO
5				0	0	Both Tcp Udp Both In Out NO

Port Blocking Schedule

☒ Always Block
 ☐ Block using an Advanced Schedule

Advanced Scheduling

Figure 91 – Port Blocking

Port blocking allows Internet traffic on specified ports, or ranges of ports to be blocked from accessing the Internet. Traffic using the specified ports will be blocked completely. This allows you to enter the name, port start, port end, protocol, and direction. Once you enter in the information click Enable and save.

Port Blocking Schedule – You may choose to block these ports all the time or Block on an Advanced Schedule.

8.1.9 Content/MIME Type Restrictions

Content/MIME Type Restrictions

Group: < Group 1 >

Enable Content/MIME Type Blocking (Global) ?

Enable Content/MIME Type Scanning YES III

Save

Block or Only Allow Content/MIME Types ?

Only Allow

Save

Content/MIME types ?

☐ Wildcard Match

+ Add

Delete Selected...

Filter...

<input type="checkbox"/> Content/MIME type	Wildcard	Actions
<input type="checkbox"/> application/json	No	
<input type="checkbox"/> test/test	No	
<input type="checkbox"/> test1/test	No	

Figure 92 – Block Content/MIME Types

This page allows you to block web content based on Content Type or MIME type. You can enter a content type like audio/mp3 to block this type of content. There are MIME type lists online that can be used for reference. You can enter wildcard matches for different file types instead of using the file extensions. For example, you can type in **audio** and check the box for Wildcard Match to block all audio type files.

You also have the choice to **Block** the entries in the list, or **Only Allow** the entries in the list.

After you enter a content/MIME type, click **Add** to add it to the list. To remove it, select it with the checkbox next to the entry and click the **Remove** button at the bottom.

8.1.10 File Extension Blocking

File Extension Blocking

Group: < Group 1 >

File Extensions

Delete Selected...

File Extension	Actions
<input type="checkbox"/> .werw	<input type="checkbox"/>
<input type="checkbox"/> .test6	<input type="checkbox"/>
<input type="checkbox"/> .dfsgdgdg	<input type="checkbox"/>
<input type="checkbox"/> .test	<input type="checkbox"/>
<input type="checkbox"/> .t1	<input type="checkbox"/>
<input type="checkbox"/> .t2	<input type="checkbox"/>
<input type="checkbox"/> .t3	<input type="checkbox"/>
<input type="checkbox"/> .t34	<input type="checkbox"/>
<input type="checkbox"/> .t345	<input type="checkbox"/>

Figure 93 – File Extension Blocking

This page allows you to block specific file extensions from being downloaded on your network.

Enter the file extension of files you would like to block in the text box below and click the **"Add"** button. You may enter a maximum of **2000** file extensions across all profiles. Each extension may be a maximum of **15** characters in length. To remove an extension from the Block list, select the extension to remove and click the **"Remove"** button located at the bottom of the page. Click the **"Done"** button when you are finished.

8.1.11 Domain Extension Restrictions

Domain Extension Restrictions

Group: < Group 1 >

Block or Only Allow Domain Extensions

Block

Save

Delete Selected...

Domain Extension	Actions
<input type="checkbox"/> .test	<input type="checkbox"/>
<input type="checkbox"/> .we	<input type="checkbox"/>

Figure 94 – Domain Extensions Restrictions

This page allows you to block or allow specific domain extensions from being accessed by a particular group. You may choose to **Block** the domain extensions in the list or to **Only Allow** the extensions in the list. If you choose to only allow the domain extensions in the list, then any domain whose extension is not in the list will be blocked. Alternatively, if you choose the block the extensions in the list, then all access to all other domain extensions will be allowed. For example, you may choose to allow only domains that end in ".com" and ".net". Any domain that does not end with those extensions will be blocked.

Enter the domain extensions in the text box below and click the **"Add"** button. You may enter a maximum of **2000** domain extensions across all profiles. Each extension may be a maximum of **15** characters in length. To remove an extension from the list, select the extension to remove and click the "Remove" button located at the bottom of the page. Click the "Done" button when you are finished.

Note: These settings do not apply to web access to direct IP addresses. You can block direct IP address access by going to Internet Controls> Block Specific Web Categories> IP Address blocking.

8.1.12 Sleep Schedule

Group: < Group 1 >

Temporary Bypass

Bypass Internet Sleep Schedule For: 1 Minute

Save

Force Sleep Schedule

Force Internet To Sleep For: 1 Minute

Save

Sleep Schedule

Select Schedule: Advanced Schedule

Advanced Schedule

Save

Figure 95 – Sleep Schedule

Internet Sleep Mode allows you to put your Internet connection to sleep (disabling all Internet traffic to and from a particular group). This is beneficial for when the Internet doesn't need to be on or accessed.

You may manually force the Internet to sleep by selecting a time period under the **"Force Internet To Sleep For:"** section and pressing the **"Sleep Now"** button. You may also bypass the sleep schedule by selecting a time period under the **"Bypass Internet Sleep Schedule For:"** section and pressing the **"Bypass Now"** button.

When manually forcing the Internet to sleep or bypassing the sleep schedule, a countdown timer will show that will allow you to cancel the forced sleep or cancel the bypass.

You may setup a daily schedule or an Advanced Schedule by which to put the Internet to sleep under the "**Sleep Schedule**" section.

When the Internet is in Sleep Mode, the "**Internet Sleep Mode**" page will be displayed in the web browser if Internet access is attempted. To customize the message that appears on the "**Internet Sleep Mode**" page, go the custom block page messages under preferences. You may override Internet Sleep Mode and wake up your Internet connection by entering the iboss login password into the "**Internet Sleep Mode**" page when it is displayed.

8.1.12.1 Sleep Mode Page

When a page is blocked from violation of the iboss sleep mode schedule, this page will show up in the web browser to the user. You may manually login and turn off Internet Sleep Mode by typing in the password and pressing Login. The Sleep Mode will continue at the next scheduled time..

8.1.13 Real-Time Monitoring/Recording

Real-time Monitoring/Recording

Group: < Group 1 >

Real-time User Activity Monitoring

Enable Real-time Activity Monitoring
☒ YES

Activity Event Count *

Activity Interval Period

Enable Video Desktop Recording
☐ NO

Enable Group VNC Password
☐ NO

Monitor the Following Categories

Ads <input type="checkbox"/> NO	Adult Content <input type="checkbox"/> NO	Alcohol & Tobacco <input type="checkbox"/> NO
Art <input type="checkbox"/> NO	Auctions <input type="checkbox"/> NO	Audio & Video <input type="checkbox"/> NO
Business <input type="checkbox"/> NO	Dating & Personals <input type="checkbox"/> NO	Dictionary <input type="checkbox"/> NO
Drugs <input type="checkbox"/> NO	Education <input type="checkbox"/> NO	Entertainment <input type="checkbox"/> NO
File Sharing <input type="checkbox"/> NO	Finance <input type="checkbox"/> NO	Food <input type="checkbox"/> NO
Forums <input type="checkbox"/> NO	Friendship <input type="checkbox"/> NO	Gambling <input type="checkbox"/> NO
Games <input type="checkbox"/> NO	Government <input type="checkbox"/> NO	Guns & Weapons <input type="checkbox"/> NO
Health <input type="checkbox"/> NO	Image / Video Search <input type="checkbox"/> NO	Jobs <input type="checkbox"/> NO
Mobile Phones <input type="checkbox"/> NO	News <input type="checkbox"/> NO	Organizations <input type="checkbox"/> NO
Political <input type="checkbox"/> NO	Porn - Child <input type="checkbox"/> NO	Porn/Nudity <input type="checkbox"/> NO
Private Websites <input type="checkbox"/> NO	Professional Services <input type="checkbox"/> NO	Real Estate <input type="checkbox"/> NO
Religion <input type="checkbox"/> NO	Search Engines <input type="checkbox"/> NO	Sex Ed <input type="checkbox"/> NO
Shopping <input type="checkbox"/> NO	Sports <input type="checkbox"/> NO	Streaming Radio/TV <input type="checkbox"/> NO
Swimsuit <input type="checkbox"/> NO	Technology <input type="checkbox"/> NO	Toolbars <input type="checkbox"/> NO
Transportation <input type="checkbox"/> NO	Travel <input type="checkbox"/> NO	Violence & Hate <input type="checkbox"/> NO
Warez <input type="checkbox"/> NO	Web Hosting <input type="checkbox"/> NO	Web Proxies <input type="checkbox"/> NO
Webmail <input type="checkbox"/> NO		

Real-time Email Alerts

Enable Email Alerts
☐ NO

Figure 96 – Real-time Monitoring/Recording

Note: The VNC recording feature is not included by default and may not be available on all models. It is a feature add-on upgrade.

This feature allows you to adjust the settings for real-time user activity monitoring feature. The iboss can monitor user activity in real-time and send email alerts, or perform desktop video recordings when a predefined level of activity is reached. This allows you to have 24/7 awareness of network activity.

User activity monitoring must be enabled for the group in order for the settings to take effect. If real-time user activity monitoring is disabled, monitoring by trigger thresholds is disabled for all computers in the group.

Real-time User Activity Monitoring – This setting enables trigger based real-time monitoring for the group. If this setting is disabled for the group, any additional options for this page have no effect.

Trigger Level And Interval – Trigger when specified number of events occur within a chosen time period.

Real-time Email Alerts – This setting will cause the iboss to send an email alert when the above threshold criteria is reached. The alert will occur when the trigger is reached to allow you to respond when certain activity is occurring.

Note: The email address that these alerts are going to be sent to can be configured below for this group or in the Settings section of the Reports interface.

Group Email Contact – This is the email where real-time alerts will be sent for activity related to the currently selected group. If left blank, the email address specified in the reporter under settings will be used for alerts related to this group. Use a semicolon between email addresses to specify more than one email address.

Send Alert When User Enters Group – This setting will cause the iboss to send an email alert whenever a user enters into this filtering group. Alerts will only be sent when a user logs in manually with override and will not be sent when a user is authenticated transparently.

Send Alert When User Leaves Group – This setting will cause the iboss to send an email alert whenever a user exits from this filtering group.

Video Desktop Recording – This setting enables a desktop recording to occur when the above threshold criteria is reached. In addition, you can specify the duration of the desktop recording.

The computer must be registered with the iboss and have VNC enabled for this setting to take effect. In addition, the computer must have a compatible VNC application installed and running. This is where you will specify how long to record the video.

Include The Following Categories – This is where you choose the categories to include in the trigger thresholds.

8.1.15 URL Lookup

URL Lookup

URL

Lookup URL

Q

Lookup URL

Submit URL for recategorization

Categories

Ads	<input type="radio"/> NO	Adult Content	<input type="radio"/> NO	Alcohol & Tobacco	<input type="radio"/> NO	Art	<input type="radio"/> NO
Auctions	<input type="radio"/> NO	Audio & Video	<input type="radio"/> NO	Business	<input type="radio"/> NO	Dating & Personals	<input type="radio"/> NO
Dictionary	<input type="radio"/> NO	Drugs	<input type="radio"/> NO	Education	<input type="radio"/> NO	Entertainment	<input type="radio"/> NO
File Sharing	<input type="radio"/> NO	Finance	<input type="radio"/> NO	Food	<input type="radio"/> NO	Forums	<input type="radio"/> NO
Friendship	<input type="radio"/> NO	Gambling	<input type="radio"/> NO	Games	<input type="radio"/> NO	Government	<input type="radio"/> NO
Guns & Weapons	<input type="radio"/> NO	Health	<input type="radio"/> NO	Image / Video Search	<input type="radio"/> NO	Jobs	<input type="radio"/> NO
Mobile Phones	<input type="radio"/> NO	News	<input type="radio"/> NO	Organizations	<input type="radio"/> NO	Political	<input type="radio"/> NO
Porn - Child	<input type="radio"/> NO	Porn/Nudity	<input type="radio"/> NO	Private Websites	<input type="radio"/> NO	Professional Services	<input type="radio"/> NO
Real Estate	<input type="radio"/> NO	Religion	<input type="radio"/> NO	Search Engines	<input checked="" type="radio"/> YES	Sex Ed	<input type="radio"/> NO
Shopping	<input type="radio"/> NO	Sports	<input type="radio"/> NO	Streaming Radio/TV	<input type="radio"/> NO	Swimsuit	<input type="radio"/> NO
Technology	<input type="radio"/> NO	Toolbars	<input type="radio"/> NO	Transportation	<input type="radio"/> NO	Travel	<input type="radio"/> NO
Violence & Hate	<input type="radio"/> NO	Warez	<input type="radio"/> NO	Web Hosting	<input type="radio"/> NO	Web Proxies	<input type="radio"/> NO
Webmail	<input type="radio"/> NO						

Figure 99 – URL Lookup

This page provides a utility to query a URL to see how it has been categorized. Once a URL has been entered and the 'Lookup' button clicked, there will be a message at the top of the screen indicating the database status of the URL. The section below will indicate which categories it is assigned.

9 Preferences

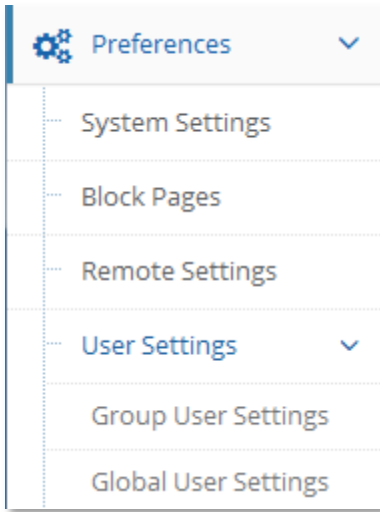


Figure 100 – Preferences

The "**Preferences**" menu allows you to choose options for configuring the current preferences of the iboss. These are the options to choose from: System Settings, Block Pages, Remote Settings, and User Settings.

System Settings – This option allows you to change the iboss system settings.

Block Pages – This option allows you to configure and customize the block pages.

Remote Management – This option allows you to setup Remote Management, to manage the iboss from anywhere.

9.1.1 System Settings

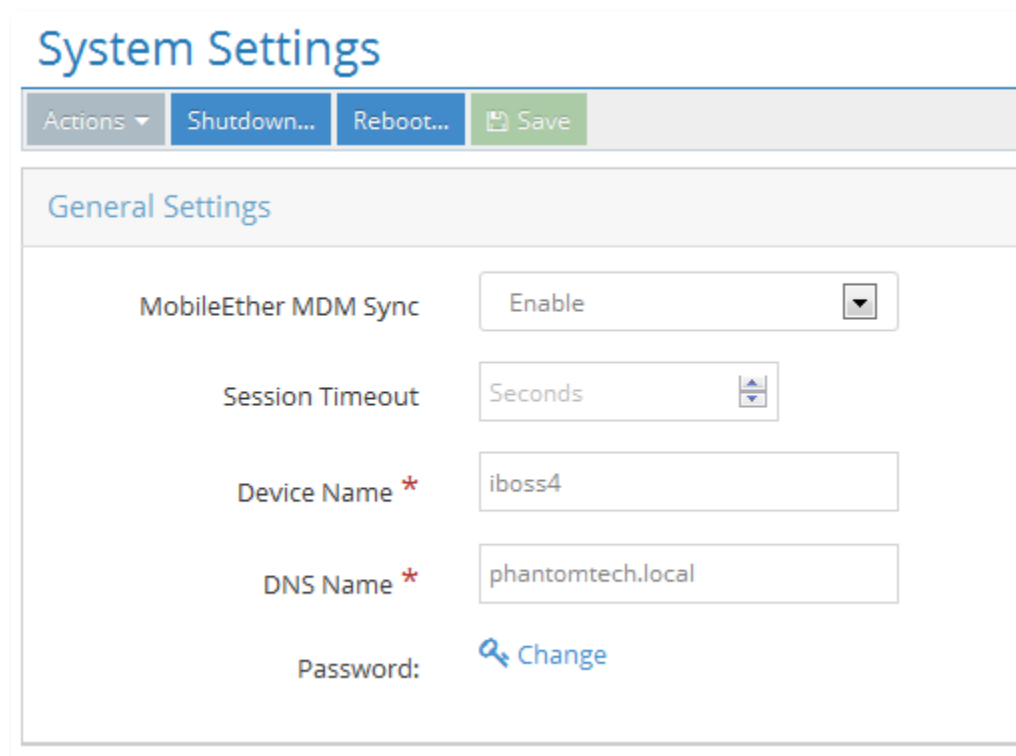


Figure 101 – System Settings

The "System Settings" page allows you to edit the device name of your iboss.

MobileEther MDM Sync – This feature allows you to sync filter settings with MobileEther MDM filter settings.

Session Timeout – The number of seconds you can be idle while managing iboss settings before you are automatically timed out. A value of 0 disables the timeout. You must choose a timeout equal to or greater than 5 minutes (300 seconds).

Device Name – This is the hostname of the iboss device.

Device DNS – This is the domain that the device is to be part of. If you use active directory, enter your domain here.

Password – You may set or change the password used for managing the iboss. The password may be a maximum of 24 characters in length.

NOTE	Be very careful with this password. It is used for configuration of your iboss and for override functions.
-------------	--

Restore Factory Defaults Action – This option allows you to set your iboss settings back to factory defaults.

Diagnostics option – This option shows diagnostic information for the iboss SWG.

You may also choose to Shutdown or Reboot the device from this page.

9.1.2 Block Pages

You may customize the pages that are displayed when a website is blocked due to its content or when the Internet is in Sleep Mode.

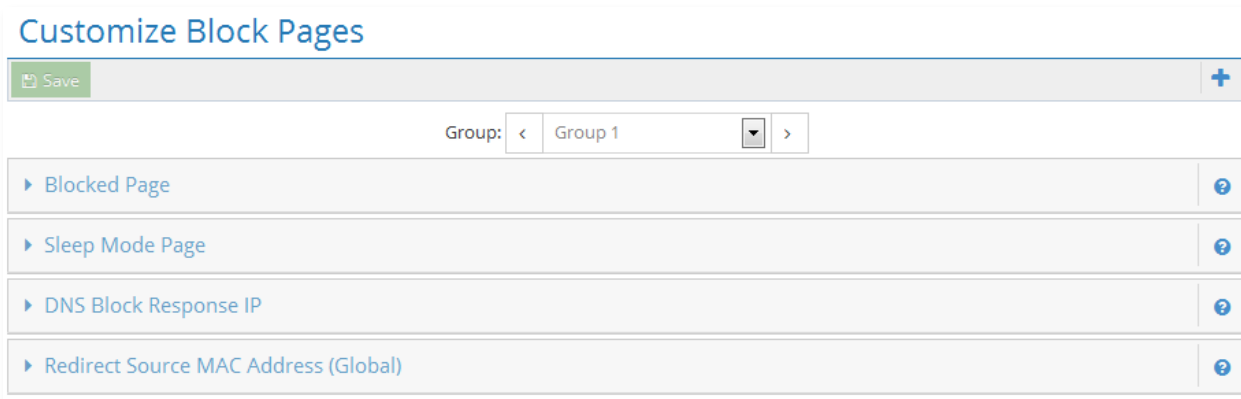


Figure 102 – Customize Block Pages

9.1.2.1 Blocked Page

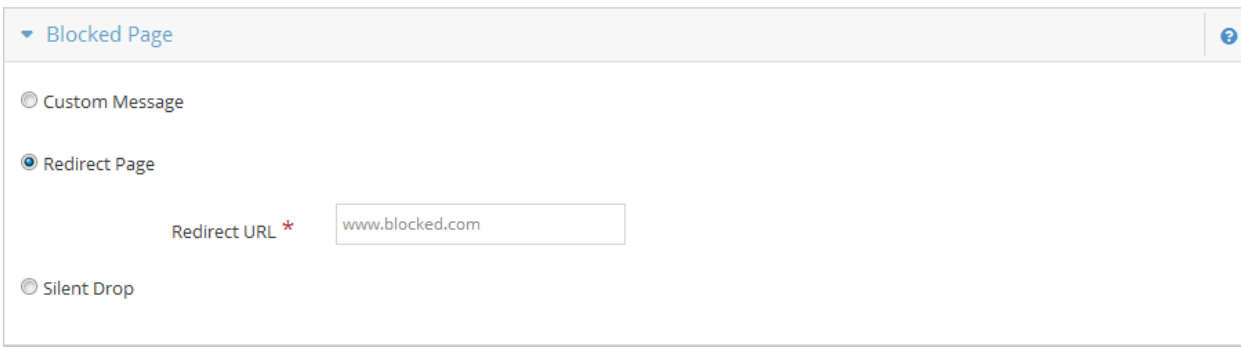


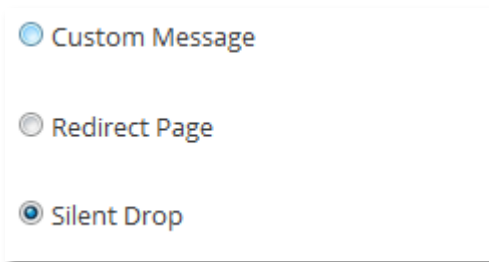
Figure 103 – Customize Block Pages – Block Page

Custom Message – This option allows you to insert a custom message into the Block Page. The custom message may be up to 299 characters in length. You may also enable or disable the Password Override feature that appears at the bottom of the page.

Redirect Page – This option allows you specify your own URL to use as the Block Page. Users will be redirected to this URL instead of the default Block Page. The URL may be up to 255 characters in length.

Silent Drop – Selecting this option will cause the iboss to silently drop violations and prevent the iboss from sending a block page response to the user when a violation occurs.

9.1.2.2 Sleep Mode Page



☐ Custom Message

☐ Redirect Page

☒ Silent Drop

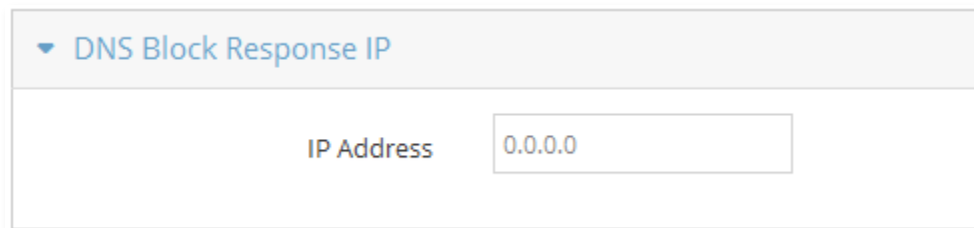
Figure 104 – Customize Block Pages – Sleep Mode Page

Custom Message – This option allows you to insert a custom message into the Sleep Mode Page. The custom message may be up to 299 characters in length. You may also enable or disable the Password Override feature that appears at the bottom of the page.

Redirect Page – This option allows you specify your own URL to use as the Sleep Mode Page. Users will be redirected to this URL instead of the default Sleep Mode Page. The URL may be up to 255 characters in length.

Silent Drop – Selecting this option will cause the iboss to silently drop the connection when the computer is in sleep mode. The user will not receive the Sleep Mode Page if this option is selected and the Internet will appear to be unavailable.

9.1.2.3 DNS Block Response IP



▼ DNS Block Response IP

IP Address

Figure 105 – Customize Block Pages – DNS Block Response IP

DNS Block Response IP – This allows you to redirect blocks that occurred via DNS to an external IP Address. Setting this value to 0 will allow the iboss to handle all DNS blocks internally.

9.1.2.4 Redirect Source MAC Address (Global)

▼

Redirect Source MAC Address (Global)

Redirect Source MAC

00:00:00:00:00:00

Figure 106 – Customize Block Pages – Redirect Source MAC Address

Redirect Source MAC Address – This allows specifying the source MAC address of the redirect packets injected by the iboss. By default the iboss uses its own MAC Address as the source within the redirect packet. This default behavior works for a majority of networks.

In rare occasions, mostly involving the optional management interface, it is necessary to specify this if the internal switch gets confused. It is recommended that this setting only be changed if you absolutely know what you're doing. Setting the value below to 00:00:00:00:00:00 disables the feature and is the default.

9.1.2.5 Block Page

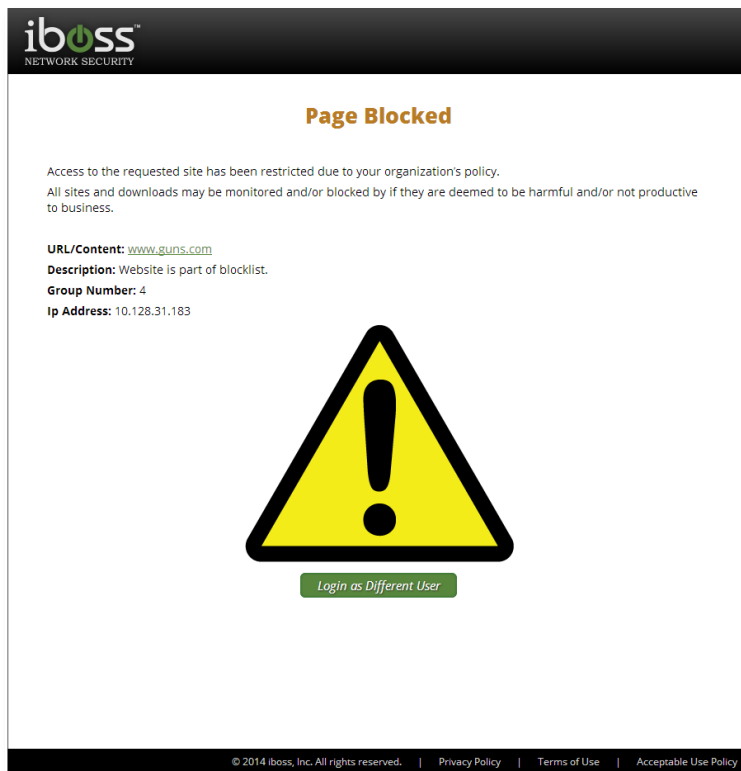
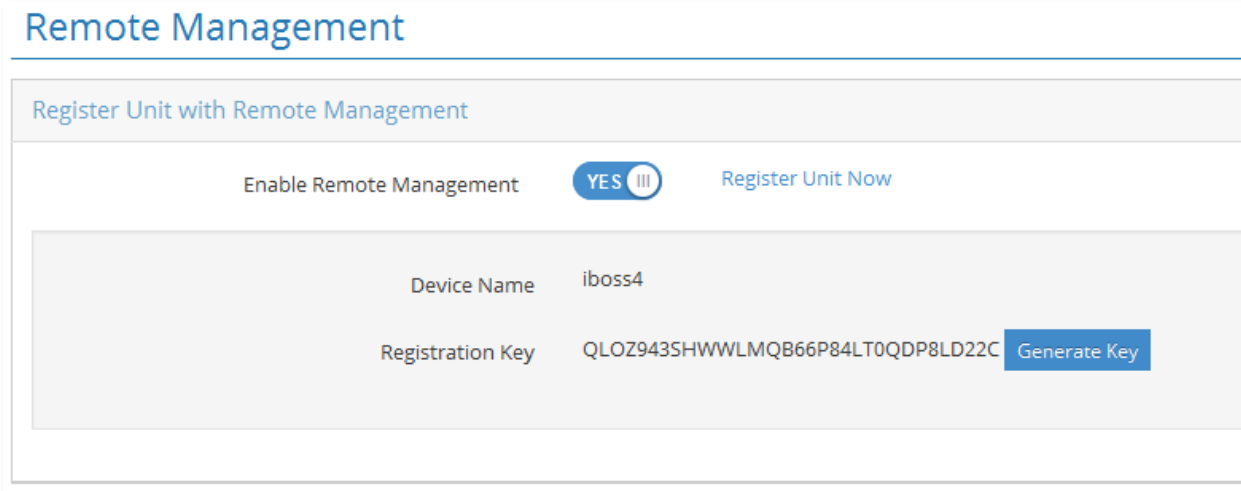


Figure 107 – iboss Block Page

When a page is blocked from a violation of the iboss settings, this page will be presented to the user. You may click the "Login as Different User" button (if present for your group) to enter yourself into a preconfigured

override group, bypassing the block in some cases. If a custom message is set, it will show up above the exclamation point.

9.1.3 Remote Management



Remote Management

Register Unit with Remote Management

Enable Remote Management **YES** ☐ Register Unit Now

Device Name	iboss4
Registration Key	QLOZ943SHWWLMQB66P84LT0QDP8LD22C Generate Key

Figure 108 – Remote Management

You may enable "**Remote Management**" which will allow you to access and manage the iboss through the web from any remote location. To enable "**Remote Management**", select the enable.

Register Unit Now – Click the "**Register Unit Now**" button below to assign this unit to a Remote Management Account. If you do not have a Remote Management Account created, you will have to create one. Registration information for this unit will automatically be transferred to simplify the registration process.

Registration Key – Each iboss holds a unique registration key used in the Remote Management registration process. This key provides security when using the Remote Management features through the web. You will be prompted for this key during the online registration process.

You may generate a new key by clicking the "**Generate Key**" button below.

Important Note: Generating a new key will remove this unit from any Remote Management account that it is currently assigned to.

9.1.4 User Settings

This section allows you to configure specific user and group settings.

9.1.4.1 Group User Settings

Save

Group: < Group 1 >

Custom Internet Access Window Company Name Logo

This allows you to add your company name or logo easily on the "Internet Access Window" when a user is logged in. The company name in text can be 50 characters and the length for the URL can be 256 characters. If you are using an image of your company logo, you can enter in the URL of where the image is hosted. The image must be in a web viewable format (ex: .gif or .jpg) and the width of "300" pixels and height of "70" pixels. If you are using the company name text, please select "Text" and enter in the company name. If you are using an image for the company logo, please select "Image" and enter in the full URL of the image.

▲ If the image you select is not at least 300 x 70 pixels, it will be stretched to this size.

Text

Image

User Login Page Type

This allows you to create a custom User Login page or choose to use the default internal user login page. If you select the redirect option, you must enter a redirect URL that points to the externally hosted user login page. This setting is applied based on the user's IP subnet default group. Typically the default user login page group is group 1. If you've defined a different default login page group to an IP subnet under Home->Setup Network Connection->Local Subnets, select the default group for that subnet on the tabs above before modifying this setting.

▲ This page must submit the same login parameters to the same form action as the default iboss login page. In addition, if the login page is located outside of the local network, you must bypass the domain in order for users to access the page.

Internal

Redirect

Advanced Settings

Custom Login Message

Custom Successful Login Message Type

Custom Text

Redirect

Use Secure HTTPS Connection When Submitting Credentials on Login Window?

No

Yes, Submit to iboss IP Address

Yes, Submit to iboss Host Name

Custom User Homepage

Figure 109 – User Settings – Group User Settings

This page allows you to configure settings for computers that require user login.

Custom Internet Access Window Company Name Logo – This allows you to add your company name or logo easily on the "Internet Access Window" when a user is logged in. The company name in text can be 50 characters and the length for the URL can be 256 characters. If you are using an image of your company logo, you can enter in the URL of where the image is hosted. The image must be in a web viewable format (ex: .gif or .jpg) and the width of "300" pixels and height of "70" pixels. If you are using the company name text, please

Version 7 — June 24, 2014

Page 137 of 159

select "Text" and enter in the company name. If you are using an image for the company logo, please select "Image" and enter in the full URL of the image.

Note: If the image that you use is not at the size of 300 x 70 it will be stretched to this size

User Login Page Type – This allows you to create a custom User Login page or choose to use the default internal user login page. If you select the redirect option, you must enter a redirect URL that points to the externally hosted user login page. This setting is applied based on the user's IP subnet default group. Typically the default user login page group is group 1. If you've defined a different default login page group to an IP subnet under Home → Setup Network Connection → Local Subnets, select the default group for that subnet on the tabs above before modifying this setting. You may choose either Internal or Redirect.

Note: This page must submit the same login parameters to the same form action as the default iboss login page. In addition, if the login page is located outside of the local network, you must ensure filtering rules allow the users to access the page.

Custom Login Message – This allows you to add a custom login message before the user logs in. This will be displayed on the user login page before they have logged in. You may type in 300 characters for the custom message.

Custom Login Message Type – This allows you to add a custom login message after the user successfully logs in. This will be displayed on the user login page before they have logged in. You may type in 300 characters for the custom message. You may also select redirect and choose the site which redirects after a successful login.

Use Secure HTTPs Connection When Submitting Credentials on Login Window – This feature allows you to select to submit credentials on the Internet Access Window securely with https to the hostname of the iboss or to the IP address of the iboss.

Custom User Homepage – This allows you to add a homepage that the users are directed to after logging in.

9.1.4.2 Global User Settings

Global User Settings

Advanced Settings

Mask Login iboss Logos ☒ NO

Manual Login User Session Heartbeat

Auto-Login User Session Timeout *

Manual Login User Session Timeout *

Save

Port Bypassing

Name Port Start Port End Both

+ Add

Delete Selected...

Filter...

<input type="checkbox"/>	Name	Port Start	Port End	Protocol	Actions
<input type="checkbox"/>	test1	10001	10002	BOTH	

Domain Bypassing

Site

+ Add

Delete Selected...

Filter...

<input type="checkbox"/>	Site	Actions
<input type="checkbox"/>	windowsupdate.com	
<input type="checkbox"/>	stancoe.org	
<input type="checkbox"/>	iboss.com	

Figure 110 – User Settings – Global User Settings

This page allows you to configure settings for computers that require user login.

Note: These settings are global across all computers that require user login and only apply to computers which require user login. These settings do not apply to identified computers which have bypass filtering rules or have a filtering group set for it.

9.1.4.2.1 Advanced Settings

Mask Login iboss Logos (Global) – This allows you to mask the iboss logos on the login pages. This hides which filtering device you are using on your network.

Manual Login User Session Heartbeat – This allows you to change how long it will take before the next heartbeat is sent to the iboss SWG from the Internet Access Window. This heartbeat is used to reset any timeouts to let the SWG know that the user is still logged in.

Auto-Login User Session Timeout (Global) – This allows you to change how long it will take before a user is automatically logged out after they have automatically been authenticated. The value is in seconds and if you are having issues with it logging out, you may set this to a higher number in seconds or set it to '0' to disable the timeout.

Manual Login User Session Timeout (Global) – This allows you to change how long it will take before a user is automatically logged out if the iboss does not hear from it being logged in. Whenever a manual user session timeout is specified under the user advanced user settings page, the timer is refreshed anytime traffic is detected going from LAN → WAN from that client. That keeps the client session alive as long as there is Internet activity from the client. In this way, even if the session activity window does not send heartbeats (for example with some mobile devices), any activity from the user keeps the session alive. If a session is set to 5 minutes, the user can surf for hours or more and whenever the user becomes idle for more than 5 minutes, the user is logged out. The value is represented in seconds and if you are having issues with it logging out, you may set it to a higher number of seconds or set it to '0' to disable the timeout.

9.1.4.2.2 Port Bypassing

This will allow you to bypass ports on computers that require user login. When a computer is set to require user login, Internet access is disabled when no user is logged into the computer. If you would like to allow access to certain ports even when a user is not logged in, you can configure them here. This is useful for programs that require port access at all times (for example, remote computer management).

9.1.4.2.3 Domain Bypassing

This will allow you to bypass domains on computers that require user login. When a computer is set to require user login, Internet access is disabled when no user is logged into the computer. If you would like to allow access to certain domains even when a user is not logged in, you can configure them here. This is useful for sites that supply updates that require access at all times (for example, Operating System & Anti-virus updates or Email access).

9.1.4.1 User Internet Access Window



The screenshot shows a window titled "Internet Access Window" with a blue header bar. Below the header is a white rectangular area containing the login form. The form has three labels: "Username:", "Password:", and "Server:". Each label is followed by a white input field. The "Server:" field has a dropdown arrow and the text "Default". To the right of the input fields is an orange button with the text "Login".

Figure 111 – Internet Access Window Login



The screenshot shows a window titled "Internet Access Window" with a blue header bar. Below the header is a white rectangular area containing session information. At the top of this area is a yellow box with a red border containing the text: "You **must** keep this window open to remain logged in. Do not forget to logout once you are finished." Below this box are three labels: "Name:", "Session Time:", and "Time Remaining:". Each label is followed by a white input field. The "Name:" field contains the text "Christopher Park". The "Session Time:" field contains the text "1 Minute". The "Time Remaining:" field contains the text "07:58 / 08:00". To the right of the input fields is an orange button with the text "Logout". At the bottom of the white area is the text "Company Name Text or Image Goes Here".

Figure 112 – Internet Access Window Session

The iboss Internet Access Window is the session window for the user that is logged in. This window must be kept open to remain logged in. This window will show you the Name of the user logged in, how long they have been

logged in (Session Time), Time Remaining/Daily time limit and which server they are logged into if you have multiple Domains. The iboss user login feature also allows you to put your own Company Name in text or put a URL for a Company Logo Image. The user login feature allows you to put custom messages before a user logs in and after they log in. This allows you to post company policies and rules before using the Internet to protect your company from liability conflicts.

10Groups

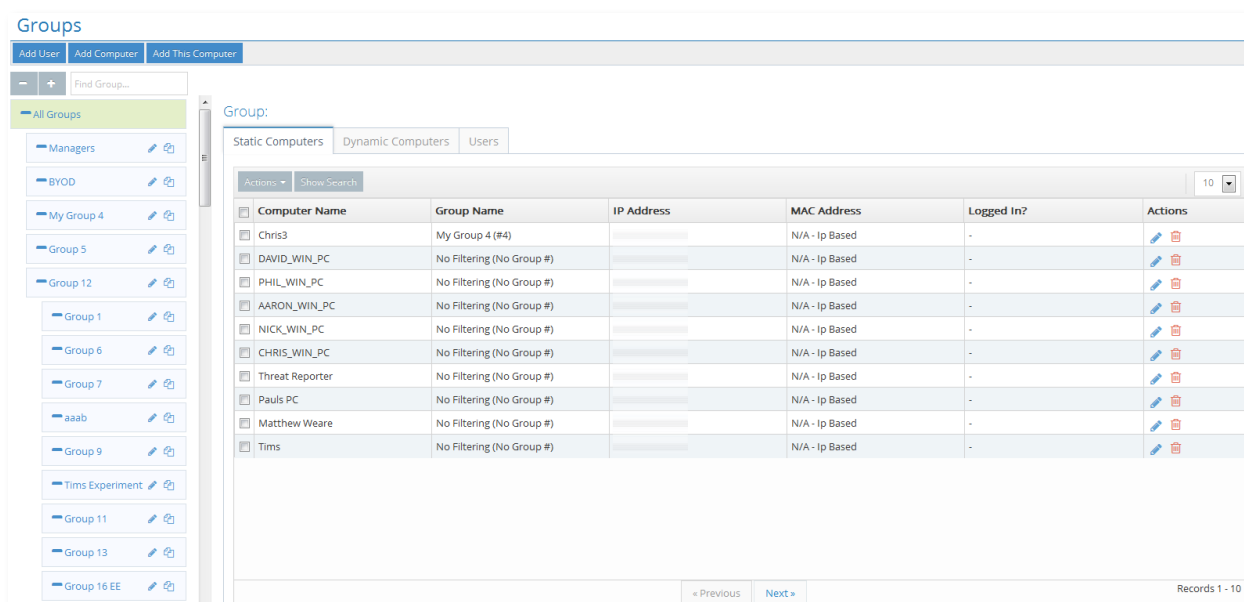


Figure 113 – Groups

This section allows you to create Groups & Users and allows you to view the users associated to the computer and the filtering groups which they fall under.

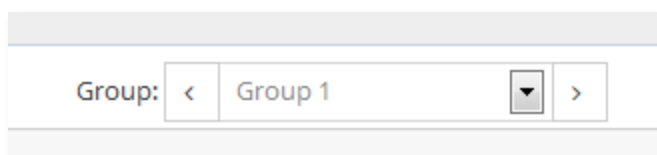


Figure 114 – Filtering Group Menu

When configuring the rules for your iboss, you will notice the Groups listed at the top of each configuration page. These pages allow you to set different filtering rules for the different filtering groups. The selected group will be selected in this drop down menu. To switch configuration for different groups, select the group in the drop down menu. You may use the arrows to go to the next or previous filtering group.

10.1 Filtering Groups



Figure 115 – Filtering Groups

This section shows the Filtering groups that are setup in the SWG filter. The Filtering groups can be created in a hierarchal format to easily group different filtering groups together. A user or computer would still only fall under one filtering group and does not inherit filtering policies from parent groups. The allowed number of filtering groups has been created for you.

Filtering groups are used to apply Internet filtering rules to computers and/or users on your network. You may customize the group names to easily identify its purpose. Group names may be up to 50 characters in length.

You can move filtering groups in the tree for easier viewing by clicking and dragging the filtering group.

10.1.1 Edit Filtering Group

The screenshot shows a dialog box titled "Edit Group #3 (Name: BYOD)". It contains the following fields and controls:

- Group Name ***: A text input field containing "BYOD".
- Alias Group Names**: A large text area for entering multiple group names.
- Logging**: A toggle switch set to "YES".
- Priority**: A numeric input field set to "3".
- Reporting Group**: A numeric input field set to "0".
- Override Group**: A toggle switch set to "NO".
- Override Timeout**: A numeric input field set to "0".
- Note**: A large text area for additional notes.
- Buttons**: "Cancel" and "Update Group" buttons at the bottom right.

Figure 116 – Edit Group

To edit the filtering group, click the pencil icon next to the filtering group name.

Group Name – You can configure the Group Name to match Security Group names or OU group names. This is determined based on your directory integration options for sending group names.

Alias Group Names – You can enter multiple group names in this field (one per line) that will match directory group names. These groups that match will be grouped together to fall under the same filtering group policy.

Logging – This option enables logging for this filtering group.

Priority – If a user matches multiple filtering groups within the iboss, the one with the highest priority number will take precedence. .

Override Group – An iboss filter group may be designated as an 'Override Group' which can be used as a method of temporarily changing to a different filtering group. This filter group should be given a priority higher than any non-Override filter groups a user may belong to. The Override Group will never be assigned via transparent login. A user presented with a block page may revalidate his/her credentials and be "bumped" up to the override group until logging out or 'Override Timeout' is reached.

Override Timeout – This timeout field will move the user back to their original filtering group when this time is reached.

NOTE This field allows you to add notes to the filtering group.

Once done configuring the settings, click the "**Update Group**" button.

10.1.2 Copy Group Settings

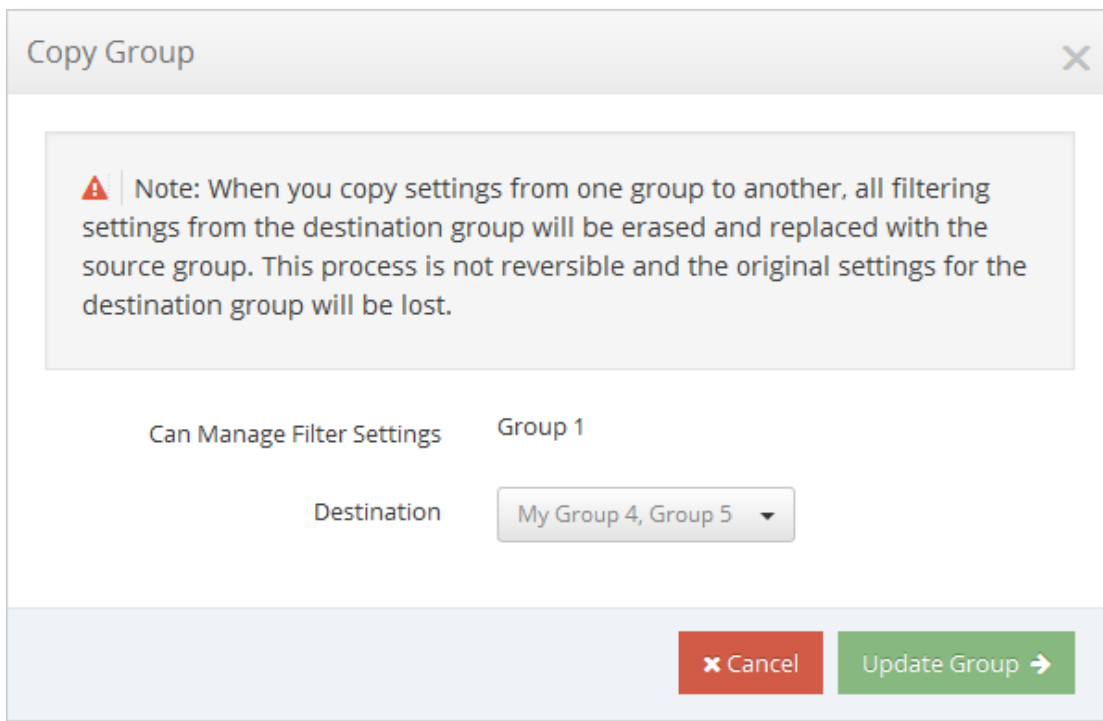


Figure 117 – Groups – Copy Group Settings

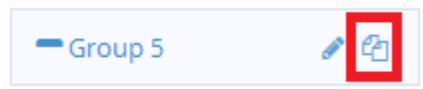


Figure 118 – Copy Group Icon

To copy group settings from one group to another, click the double document icon to pull up the Copy Group Settings.

The Copy Group window allows you to quickly copy filtering settings from one group to another, or several. Select the group to copy settings from and a group to copy settings to and then click the Update Group button. This will completely overwrite the destination and provides a configuration starting point but there is no connection between the groups from this point.

NOTE

This process is not reversible and the original settings for the destination group will be lost.

10.1.3 Group – Computers & Users Tabs

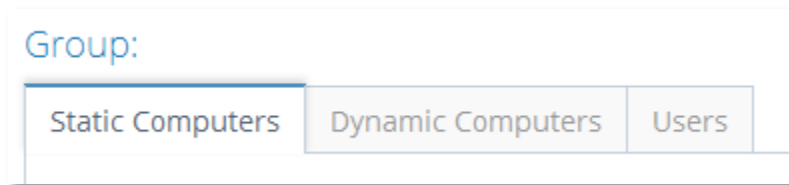


Figure 119 – Group – Computers & Users Tabs

The Groups section has tabs at the top to switch from Static Computers, Dynamic Computers, and Users for each select group or All Groups.

Static Computers – The computers listed under the Static Computers are Manually Identified Computers and fall under the filtering group that is selected..

Dynamic Computers – The computers listed under the Dynamic Computers are computers that have been detected going through the iboss and fall in the filtering group that is selected.

Users – The users listed under the Users tab are Users that have been manually added to the SWG and assigned to the filtering group that is selected.

10.1.1 Add User

The screenshot shows the 'Add User' dialog box. The 'General' tab is active, displaying various user configuration fields. The 'Type' dropdown is set to 'User'. The 'User' field is marked with a red asterisk and is currently empty. The 'Authenticate via LDAP' toggle is set to 'NO'. The 'Password', 'First Name', and 'Last Name' fields are empty. The 'Session Timeout' field is empty with a spinner icon. The 'Note' field is a large empty text area. The 'Apply Filtering Group' dropdown is set to 'BYOD'. At the bottom right, there are two buttons: 'Close' (red) and 'Add User' (green with a right arrow).

Figure 120 – Add User

To add a new user, click the Add User button at the top.

These users will not have access to the iboss settings and cannot log onto the iboss to change settings unless “**Delegation Settings**” are enabled.

10.1.1.1 General

Type – You can select User or Admin Login AD/LDAP Group. Selecting Admin Login AD/LDAP group allows administrator logins to the iboss from an AD or LDAP group.

User – Enter the username or group name in this User field.

Authenticate via LDAP – You can enable this option to authenticate the user via LDAP to use the user's password within LDAP.

Password – Set the password for the user if you do not have Authenticate via LDAP option selected.

First Name – Enter the user's first name.

Last Name – Enter the user's last name.

Session Timeout – Enter the amount of minutes until the user is logged out of the Internet Access Window. The default is 0 which will not log the user out automatically with this option.

Note – This allows you to enter a note for the user.

Apply Filtering Group – This option allows you to specify which group the user will fall under when they authenticate. You can also select No Filtering which is the last option to bypass filtering for this user.

10.1.1.2 Delegation

The screenshot shows the 'Add User' dialog box with the 'Delegation' tab selected. The settings are as follows:

- Settings Administrator:** YES (selected)
- Administrator Type:** Delegated
- Permissions:** None selected
- Filter Settings Group Access:** None selected
- Default Management Group:** BYOD

Buttons at the bottom: Close, Add User →

Figure 121 – Users – Delegation

When adding a user to the iboss, you will also have options to give them access to filtering settings.

Settings Administrator – Option to enable delegated administration.

Administrator Type – Full allows full access to the iboss SWG Filter. Delegated allows you to specify which permission settings and which groups the user can manage.

Permissions – Select which filter control settings the user is allowed to manage. You can select multiple settings.

Filtering Settings Group Access – Select which filtering groups the user is allowed to manage.

Default Management Group – This is the default management group that the user is administering.

10.1.1.3 Time Limits

The screenshot shows a web-based 'Add User' dialog box with a close button (X) in the top right corner. It has three tabs: 'General', 'Delegation', and 'Time Limits', with 'Time Limits' currently selected. Inside the 'Time Limits' tab, there is a section titled 'Remaining Time Today' with a blue 'Reset Time Limits' button. Below this, there are six rows representing the days of the week from Tuesday to Sunday. Each row contains a dropdown menu currently set to 'Unlimited' and a blue horizontal progress bar. At the bottom of the dialog, there are two buttons: a red 'Close' button and a green 'Add User' button with a right-pointing arrow.

Figure 122 – Users – Time Limits

This will allow you to set daily time limits for each day of the week for a user. You can set a time between 15 minutes to 23 hours that a user can be logged in from throughout the day. This means that when a user has the allocated time throughout the day to use the time limit. When finished click the "**Add User**" button. If you want to cancel your changes click the "**Close**" button.

10.1.2 Add Computer

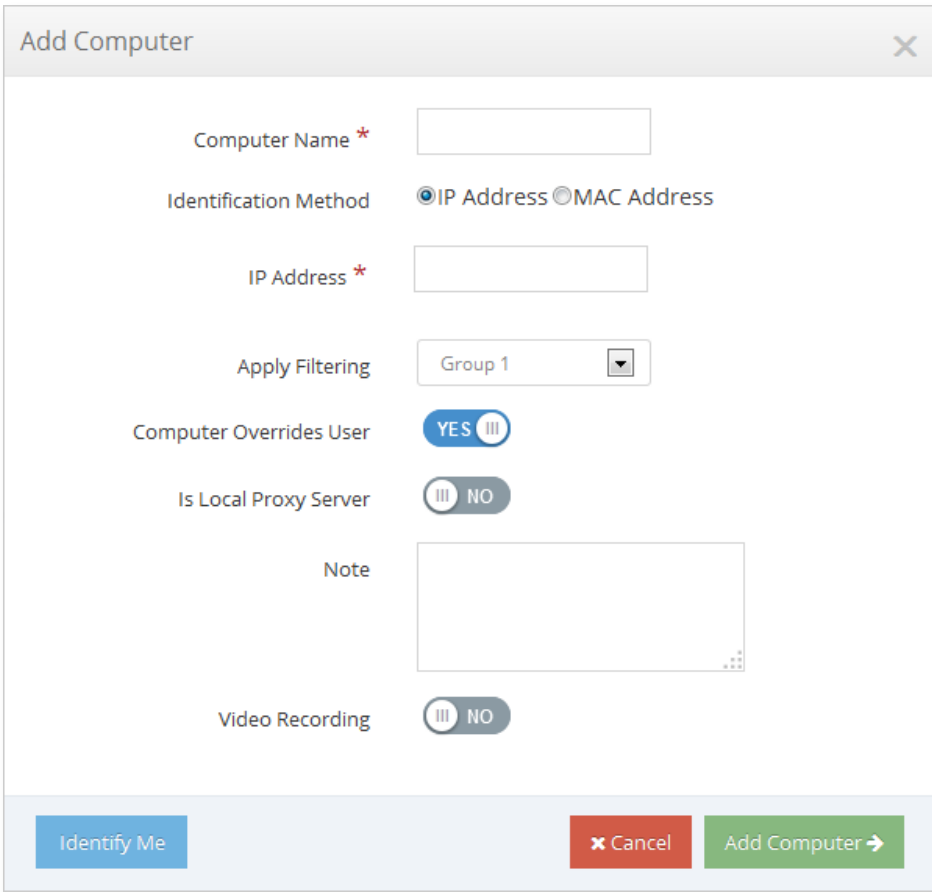


Figure 123 – Add Computer

To identify the computer you are using now, click the **"Add this computer"** button. Advanced users may click the **"Add Computer"** button to manually identify a computer. For the **"Add Computer"**, you will need to know the IP address or MAC address of the computer you wish to identify.

Computer Name – Enter a Computer Nickname for your reference.

IP Address / MAC Address Type – If you have your local subnets setup to identify your subnet as IP address, choose IP address. MAC Addresses may not be visible to the iboss on a layer 3 routed network with internal gateways and multiple subnets.

IP Address – Enter the IP address

Apply Filtering – You may either set the Apply Filtering to **"Yes, Use Default Rules"** with one of the filtering groups, **"No, Bypass Filtering Rules"** or **"Require user login for this computer"** for the computer you are identifying.

*The "Yes, Use Default Rules" will show the assigned name of the filtering group.

Computer Overrides User – This option allows you to enforce the specified filtering policy on that computer, regardless of the rights of the person logged in.

Is Local Proxy Server – This option is to identify if the computer you are identifying as a proxy server on your local network.

Video Recording – *There are more options if you have the DMCR feature added. This will allow you to put the Port, Password and IP address of the client VNC computer. Please refer to the Controls → Monitoring section for more information.

When finished click the "Add Computer" button. If you want to cancel your changes click the "Cancel" button.

11 Tools

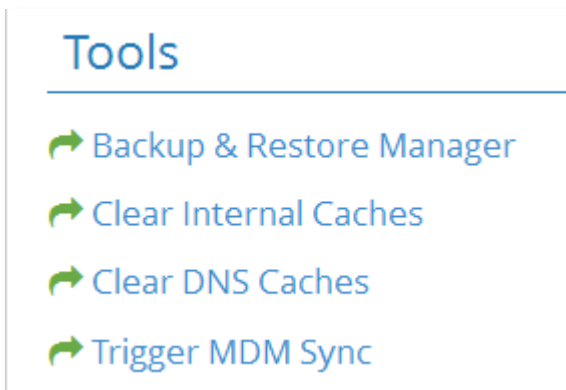


Figure 124 – Tools

This section has quick links for the Backup & Restore Manager, Clear Internal Caches, Clear DNS Caches, and Trigger MDM Sync.

11.1 Backup & Restore Manager

 A screenshot of a login form titled 'Backup Manager Login'. The form has a light gray header with the title. Below the header, there is a 'Password:' label followed by a text input field. To the right of the input field is a blue 'Login' button.

Figure 125 – Backup & Restore Manager Login

The login for this interface requires the full admin password to login.

Restore Points

+ New Restore Point

Filter...









Name	Automated Restore Point	Description	Actions
TEST	No	TEST	 
Base-Settings	No		 
Restore	No		 
Auto_iBoss_Restore_TEST4_06...	Yes	Automated Restore Point	 

Figure 126 – Backup & Restore – Restore Points & Creating Restore Point

Once you login, you can see all the restore points that have been created. There are no restore points created by default. It is recommended to create a restore point after you have configured your controls settings and then click the Download button to copy the restore point off of the device.

When a restore point is created, you have the option to delete it off the device, download the restore point which contains all of the settings and firmware, and the option to restore the iboss device back to a specific Restore Point.

Restoring the iboss from a restore point must be from the same model of the iboss. It does revert back to the firmware version number that the iboss was on when the restore point was created.

If you have multiple iboss devices and would like to copy settings from one device to another, one thing to note is that the subscription key also gets copied and restored. This may overwrite your current subscription key for the second unit. If this is the case, you will want to save the restore point of the second iboss device and after restoring an imported restore point, overwrite the subscription key with the original subscription key that was there prior.

Backup Manager

Logoff
Save

Backup Settings

Backup Status

Status Restore point creation successfully finished
at: Tue Jun 24 09:31:23 PDT 2014

Last Run Date Tuesday, June 24, 2014

Next Run Date Wednesday, June 25, 2014

Automated Backup Schedule

☐ Disabled
☒ Roll Logs Daily at 9:30 AM
☐ Roll Logs Weekly on at 9:30 AM
☐ Roll Logs on day of every month at 9:30 AM

Backup Folder Settings

Backup to SMB Share ☐ NO

Email Status Alerts

Send Backup Alerts ☐ NO

Figure 127 – Automated Scheduled Backup

You can setup a schedule to create a restore point of the settings on a daily, weekly, or monthly schedule. This saves a restore point onto the iboss device.

Backup Folder Settings – You can save these scheduled restore point backups to a SMB Share folder. You will want to enable this feature and setup the folder path and authentication settings.

Email Status Alerts – These options will allow you to use an SMTP server to email you when a backup was successfully run.

Restore Points		
<div> <div>+ New Restore Point</div> <div>Filter...</div> </div>		
Name	Automated Restore Point	Description
TEST	No	TEST
Base-Settings	No	
Restore	No	
Auto_iBoss_Restore_TEST4_06...	Yes	Automated Restore Point

Download Restore Point

Download

Delete

Download

Delete

Download

Delete

Download

Delete

Figure 128 – Restore Settings

This option allows you to import a restore point into the device. This is handy if you'd like to copy settings from one device to another, or if you have an onsite spare device and have automated backups running and need to restore to a backed up restore point.

To restore to a backup, click **Browse** and find the .ibrp backup file for the restore point and click **Import**. This will add it to the list of Restore points at the top of this page. When you are ready, click the **Restore** button next to the Restore point which will reboot the device and load this restore point.

11.2 Clear Internal Caches

This option will clear all cached usernames to filtering groups used with the AD Logon Scripts. It will also clear any signature matches for applications that have been detected based on signature footprint.

11.3 Clear DNS Caches

This option will clear all DNS Caches. It is not recommended to clear this during business hours as this will dissociate domains to IP addresses for more accurate identification of sites.

11.4 Trigger MDM Sync

This option syncs the settings with the MDM MobileEther. This feature would need to be enabled on the iboss under Home → Preferences → System Settings. This option would also need to be enabled on the iboss Enterprise Reported and integrated with the MDM MobileEther interface.

12Firmware Updates

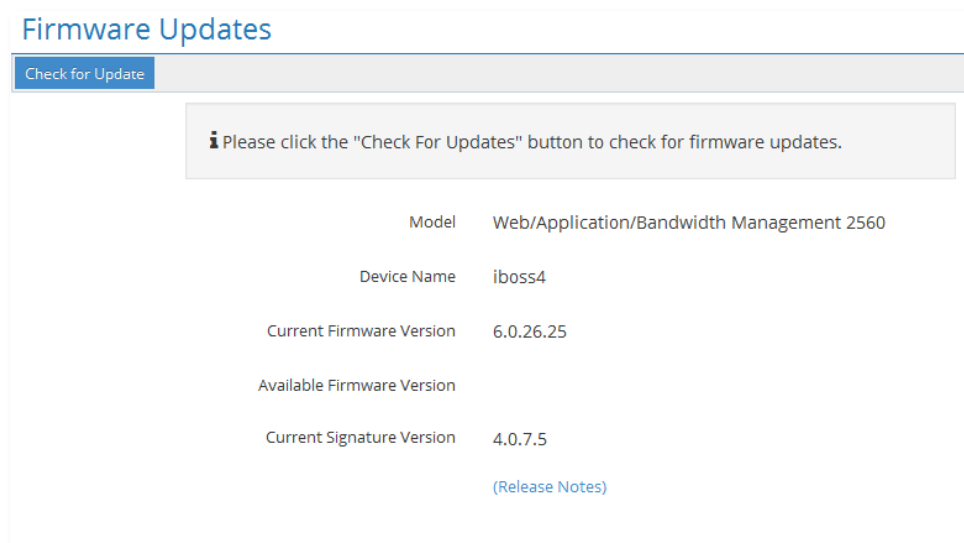


Figure 129 – Firmware Updates

Firmware updates are published as needed. The updates are downloaded over the Internet directly into the device. Firmware updates include feature enhancements only and are not related to the iboss Internet filtering functionality. The iboss will always be up-to-date with the latest web category URLs and online application definitions used with filtering rules. You must have an active subscription and a live Internet connection in order to download firmware updates.

Model – Indicates the model of your iboss device.

Device Name – Indicates the name given to the iboss.

Current Firmware Version – Indicates the firmware version installed on your iboss.

Available Firmware Version – Indicates the latest firmware version available for download. If this version number matches the number in the "Current Version" field, then your iboss firmware is up to date.

Current Signature Version – Indicates the signature version installed on your iboss

Check for Update button – The "Download/Install" button will appear when new firmware is available after clicking Check for Updates. Click this button to begin downloading and installing the new firmware. The **"Install"** button will appear when new firmware has been downloaded and is ready to install. Click this button to begin installing the new firmware. Once this process begins, do not power down the iboss until installation is complete. When the installation is complete, you will be redirected back to the iboss home page.

Download Progress – Indicates the download progress of the firmware updates.

13Subscription

Subscription

Trigger Subscription Check

Subscription status

This page allows you to view your subscription status and add or update a Subscription Key. An active Subscription Key must be registered in order for the iboss to function.

Subscription Information

Model	Web/Application/Bandwidth Management 2560		
Current PUDSUS Url	https://pudsus1.ibossconnect.com		
Subscription Status	Last subscription checks successful.		
Primary Subscription Key		<a>Edit Primary Key	
Primary Subscription Status	Active		
Primary Subscription Expiration			
Malware Subscription Key		<a>Edit Malware Key	
Malware Subscription Status	Unknown		
Malware Subscription Expiration			

Figure 130 – Subscription

The iboss requires an active subscription to function. The unit may already be pre-activated when you receive it, or you may need to obtain and/or activate a subscription key and register the active subscription key with your iboss.

14Support

This section brings you to helpful links on our website for links to our knowledgebase, support center, iboss university videos, contact information and more.

Please refer to this updated links for updated information regarding support.

15Troubleshooting

15.1 Password Recovery

In the event that the iboss administration password becomes lost, please contact iboss support for help retrieving it.

15.2 Resetting to Factory Defaults

The iboss can be reset back to factory default settings through two different methods. After performing the factory reset, all of the iboss settings will be set back to default values (including Internet connection, Internet filtering and password settings).

15.2.1 Through the iboss User Interface

Login to iboss Interface, click on Preferences → System Settings → Actions → Restore Factory Defaults. You will be prompted to confirm before continuing.

15.2.2 Using the iboss Console Port

Connect your computer to the console port of the iboss. (Please see console setup in this manual for more information on connecting the iboss to the console port). Choose the option Restore Factory Defaults. Confirm that you would like to reset the factory defaults.

15.3 Technical Support

iboss prides itself on supporting our products and services for our customers. Please use the information below if you are in need of assistance.

Website Support: <http://support.iboss.com>

Telephone Support: 1.858.568.7051 option 3

E-mail Support: support@iboss.com

16 APPENDIX

16.1 Terms of Use

BY PROCEEDING TO USE THE PRODUCTS AND SERVICES PROVIDED BY IBOSS, INC. YOU ACKNOWLEDGE YOUR AGREEMENT TO BE BOUND BY THE FOLLOWING TERMS AND CONDITIONS AVAILABLE AT:

<http://www.iboss.com/termsfuse/index.html>

IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MAY NOT USE THE PRODUCTS AND SERVICES PROVIDED BY IBOSS INC.

For the latest news, features, documentation and other information regarding the iboss please visit:

<http://www.iboss.com>

17 REGULATORY STATEMENT

FCC

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC rules.

CE

This equipment has been tested and found to comply with the limits of the European Council Directive on the approximation of the law of the member states relating to electromagnetic compatibility (89/336/EEC) according to EN 55022 Class B.

FCC and CE Compliance Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment.